Electronic Evidence in Criminal Investigations and Actions:

Representative Court Decisions and Supplementary Materials

Ronald J. Hedges, Editor

APRIL 2022

Table of Contents

FOREWARD TO THE APRIL 2022 EDITION vii

TAGS viii

ABBREVIATIONS ix

DECISIONS – UNITED STATES SUPREME COURT 1

Andrews v. State, No. 20-937, *cert.* denied (U.S. May 17, 2021), decision below, *State v. Andrews*, 243 N.J. 447 (2020) 1

Caniglia v. Strom, No. 20-157, 2021 WL 1951784 (U.S. May 17, 2021) 1

City of Tahlequah v. Bond, No. 20-1668, 2021 WL 4822664 (U.S. Oct. 18, 2021) (*per curiam*) 2

Lange v. California, No. 20-18, 2021 WL 2557068 (U.S. June 23, 2021) 4

Merchant v. Mayorkas, No. 20-1505, *cert.* denied, 2021 WL 2637881 (U.S. June 28, 2021), decision below, *Alasaad v. Mayorkas,* 988 F.3d 8 (1st Cir. 2021) 4

Rivas-Villegas v. Cortesluna, No. 20-1539, 2021 WL 4822662 (U.S. Oct. 18, 2021) (*per curiam*) 4

Van Buren v. United States, No. 19-783, 2021 WL 2229206 (U.S. June 3, 2021) 7

DECISIONS – FEDERAL 7

In re Capitol Breach Grand Jury Investigations Within the District of Columbia, Grand Jury Action No. 21-20 (BAH), 2021 WL 3021465 (D.D.C. July 16, 2021) 7

Harbor Healthcare System, L.P. v. United States, No. 19-20624, 2021 WL 3009732 (5th Cir. July 15, 2021) (*per curiam*) 8

Mexican Gulf Fishing Co. v. U.S. Dep't of Commerce, Civil Action No. 20-2312, 2022 WL 594911 (E.D. La. Feb. 28, 2022) 9

Project Veritas Action Fund v. Rollins, Nos. 19-1586, 19-1640, 2020 WL 7350243 (1st Cir. Dec. 15, 2020), *cert.* denied, No. 20-1598, 2021 WL 5434360 (U.S. Nov. 22, 2021) 10

I/M/O Search of Information That Is Stored at the Premises Controlled by Google LLC, Case No. 21-SC-3217 (GMH), 2021 WL 6196136 (D.D.C. Dec. 30, 2021) 12

I/M/O Search of Information that is Stored at the Premises Controlled by Google, LLC, Case No. 21-MJ-5064-ADM, 2021 WL 2401925 (D. Kan. June 4, 2021) 14

In re Search Warrants Executed on Apr. 28, 2021, 21-MC-425 (JPO), 2021 WL 2188150 (S.D.N.Y. May 28, 2021) 14

United States v. Bebris, No. 20-3291, 2021 WL 2979520 (7th Cir. July 15, 2021) 15

United States v. Caesar, No. 19-3961, 2021 WL 2559471 (3d Cir. June 23, 2021) 16

United States v. Chatrie, Criminal Case No. 3:19cr130, 2022 WL 628905 (E.D. Va. Mar. 3, 2022) 17

United States v. Dennis, 20 Cr. 623 (LGS) (S.D.N.Y. Jan. 26, 2022) 18

United States v. Fleury, No. 20-11037, 2021 WL 5933789 (11th Cir. Dec. 16, 2021) 18

United States v. Holmes, Case No. 5:18-cr-00258-EJD-1, 2021 WL 3395146 (N.D. Ca. Aug. 3, 2021).... 22
United States v. Hunt, 21-CR-86 (PKC), 2021 WL 1428579 (E.D.N.Y. Apr. 15, 2021).... 23
United States v. Johnson, No. 19-4331, 2021 WL 1703605 (4th Cir. Apr. 30, 2021).... 24
United States v. Korf, No. 20-14223, 2021 WL 3852229 (11th Cir. Aug. 30, 2021) (*per curiam*).... 27
United States v. Lamm, No. 20-1128, 2021 WL 3196472 (8th Cir. July 29, 2021).... 28
United States v. Meals, No. 20-40752, 2021 WL 6143550 (5th Cir. Dec. 30, 2021).... 29
United States v. Moore-Bush, 982 F.3d 50 (1st Cir. 2020), granting pet. for en banc rehearing and vacating judgment of panel below.... 29
United States v. Moses, 6:19-CR-06074 EAW, 2021 WL 4739789 (W.D.N.Y. Oct. 12, 2021).... 29
United States v. Ramirez-Mendoza, No. 4:20-CR-00107, 2021 WL 4502266 (M.D. Pa. Oct 1, 2021).... 30
United States v. Oliver, 987 F.3d 794 (8th Cir. 2021).... 31
United States v. Tuggle, No. 20-2352, 2021 WL 2946100 (7th Cir. July 14, 2021).... 33
United States v. Wilson, No. 18-50440, 2021 WL 4270847 (9th Cir. Sept. 21, 2021).... 34
Villarreal v. City of Laredo, No. 20-40359, 2021 WL 5049281 (5th Cir. Nov. 1, 2021).... 36
DECISIONS – STATE.... 36
City of Seattle v. Buford-Johnson, No. 81627-6-1, 2021 WL 6112342 (Wash. Ct. App. Div. 1 Dec. 27, 2021).... 36
Commonwealth v. Carrasquillo, SJC-13122 (Mass. Feb. 7, 2022).... 37
Commonwealth v. Davis, 487 Mass. 448, 168 N.E.3d 294 (2021).... 38
Commonwealth v. Delgado-Rivera, 487 Mass. 551, 168 N.E.3d 1083 (2021).... 41
Commonwealth v. Yusuf, 488 Mass. 379 (2021).... 42
Ex Parte Jones, No. PD-0552-18, 2021 WL 2126172 (Tex. Ct. Crim. App. May 26, 2021).... 43
People v. Blanco-Ortiz, 2021 NY Slip Op 04447 (App. Div. 4th Dept. July 16, 2021) (mem.).... 44
People v. Sneed, 2021 IL App (4th) 210180 (Nov. 18, 2021).... 44
State v. Acosta, 311 Or. App. 136, 489 P.3d 608 (2021).... 48
State v. Burch, 2021 WI 68 (2021).... 49
State v. Caronna, Docket Nos. A-0580-20 & A-0581-20 (N.J. App. Div. Nov.3, 2021).... 52
State v. Carrion, A-14-20 (N.J. Sup. Ct. Dec. 27, 2021).... 52
State v. Dawson, 340 Conn. 136 (Conn. 2021).... 54
State v. Katz, Supreme Court Case No. 20S-CR-632, 2022 WL 152487 (Ind. Jan. 18, 2022).... 54
State v. Martinez, No. 13-20-00169-CR (Tex. 13th Dist. Ct. App. Jan. 20, 2022).... 55
State v. McQueen, No. A-11-20 (N.J. Sup. Ct. Aug. 10, 2021).... 55
State v. Smith, No. SC99086 (Mo. Jan. 11, 2022) (en banc).... 56

In Interest of Y.W.-B., J-39A&B-2021, 2021 WL 6071747 (Pa. Dec. 23, 2021) 57

DECISIONS – FOREIGN 58

Big Brother Watch v. United Kingdom, Apps. Nos. 58170/13, 62322/14 and 24960/15 (European Ct. of Human Rights: May 25, 2021) 58

Press Release, *EDPS Orders Europol to Erase Data Concerning Individuals with No Established Link to a Criminal Activity* (Jan. 10, 2022) 58

STATUTES, REGULATIONS, ETC. – FEDERAL 59

"2020 Wiretap Report: Intercepts and Convictions Decrease" (United States Courts: June 28, 2021) 59

#Discovery Materials 59

#Fourth Amendment – Warrant Required or Not 59

#Miscellaneous 59

General Accounting Office, "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," GAO-21-518 (June 2021) 59

Department of Justice, "Body-Worn Camera Policy" (Office of the Deputy Attorney General: June 7, 2021) 59

Department of Justice, "Cellular Analysis & Geo-Location Field Resources Guide" (FBI CAST: Current as of Mar. 2019) 59

Department of Justice, "Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities" (Office of Public Affairs: Apr. 13, 2021) 60

Department of Justice, "United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime" (Office of Public Affairs: Dec. 15, 2021) 60

C.A. Theohary, "Use of Force in Cyberspace," *In Focus* (Cong. Research. Serv.: Dec. 10, 2021) 60

STATUTES, REGULATIONS, ETC. – STATE 60

Office of the Inspector General, "The Chicago Police Department's Use of Shotspotter Technology" (City of Chicago: Aug. 24, 2021) 60

"Protecting Household Privacy Act," Pub. Act 102-0597 (Illinois: Enacted Aug. 27, 2021, eff. date Jan. 1, 2022) 61

"An Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials," L.D. 1585 (Maine: Enacted June 30, 2021, eff. date Oct. 1, 2021) 61

ARTICLES 61

J. Bambauer, "Geofence Warrants are the Future (and That's a Good Thing," *The Volokh Conspiracy* (Mar. 16, 2022) 61

T. Brewster, "Cops Demand Google Data on Anyone Who Searched a Person's Name … Across a Whole City," *Forbes* (May 17, 2017) 61

T. Brewster, "Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address, and Telephone Number," *Forbes* (Oct. 4, 2021) 62

B.D. Brown, "Why Did the Trump DOJ Secretly Seize Phone Records from *Post* Journalists?" *Columbia J. Review* (May 12, 2021) 62

J. Cox, "FBI's Backdoored Anom Phones Secretly Harvested GPS Data Around the World," *Motherboard* (Jan. 4, 2022) 62

H.B. Dixon, Jr., "Cell Phones, Social Media, and the Capitol Insurrection," *Judges' Journal* (ABA: Apr. 21, 2021) 62

R. Fausset & G.M. Nieto del Rio, "As Body Cameras Become Commonplace, a Debate Over When to Release the Footage," N.Y. Times (May 2, 2021) 63

C. Fennessy, "A Multilateral Surveillance Accord: Setting the Table," *Lawfare* (Lawfare Institute: Apr. 23, 2021) 63

J. Garland, *et al.,* "Federal Court Expresses Skepticism About Validity of Geofence Warrants But Declines Suppression Remedy," *Covington Inside Privacy* (Mar. 9, 2022) 63

S. Goldenberg & J. Anuta, "Adams Eyes Expansion of Highly Controversial Police Surveillance Technology," *Politico* (Feb. 8, 2022) 64

S. Gordon, "DC Court Is Wrong on Jan. 6 Grand Jury Evidence Sharing," *Law360* (July 30, 2021) 64

P.W. Grimm, M.R. Grossman & G.V. Cormack, "Artificial Intelligence as Evidence," 19 *Nw. J. Tech. & Intell. Prop.* 9 (2021) 64

P.W. Grimm, "New Evidence Rules and Artificial Intelligence," *Litigation*, Vol. 45, No.1 (ABA: Fall 2018) 64

S. Holder & F. Akinnibi, "Suburbs of Surveillance," *Bloomberg CityLab* (Aug. 4, 2021) 65

V. Hughes, "Two New Laws Restrict Police Use of DNA Search Methods," *N.Y. Times* (May 31, 2021) 65

A. Iftimie, "No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims," *Lawfare* (Apr. 19, 2021) 65

A. Kabaria & J.D. Seiver, "Illinois 'Protecting Household Privacy Act' Takes Effect," *Privacy & Security Law Blog* (Davis Wright Tremaine LLP: Jan. 13, 2022) 65

O.S. Kerr, "The Fourth Amendment and Geofence Warrants: A Critical Look at *United States v. Chatrie," The Volokh Conspiracy* (Mar. 11, 2022) 66

O.S. Kerr, "The Fourth Amendment Limits of Internet Content Preservation," 65 *St. Louis Univ. L. J.* 753 (2021) 66

M. MacCarthy, "Mandating Fairness and Accuracy Assessments for Law Enforcement Use of Facial Recognition Systems," *TechTank* (Brookings: May 26, 2021) 66

R. Mann, "Diverse Six-Justice Majority Rejects Broad Reading of Computer-Fraud Law," *SCOTUSblog* (June 3, 2021) 66

M. Mermelstein, S. Frase & A. Epperson, "Overbroad Searches and Seizures: Google Customer Data Stored Outside of Gmail," *Litigation J.* 49 (ABA: fall 2021) 67

N. Mott, "FBI Document Shows How Popular Secure Messaging Apps Stack Up," *PC* (Nov. 29, 2021) 67

J. Nash, "Fingerprint Biometrics Still a Solid Tool for Police – Despite Persistent Myths," *BIOMETRIC Update.Com* (Nov. 17, 2021) 67

C.F. Ortiz & K. Suominen, "DOJ and IRS' Analysis of Crypto Records and Work with Private Experts and International Partners Leads to Arrest," *Tax Controversy 360* (Apr. 30, 2021) 67

S.M.G. Rankin, "*Technological Tethereds:* Potential Impact of Untrustworthy Artificial Intelligence in Criminal Justice Risk Assessment Instruments," 78 *Wash. & Lee L. Rev.* 647 (2021) 68

T. Riley, "Feds' Spending on Facial Recognition Tech Expands, Despite Privacy Concerns," *Cyberscoop* (Jan. 10, 2022) 68

S. Rippy & N. Sakin, "Van Buren: The Implications of What is Left Unsaid," *Privacy Advisor* (IAPP: June 18, 2021) 68

S.W. Smith, "The Cell Phone Donut Hole in the Tracking Device Statute," 14 *Fed. Cts. L. Rev.* 1 (FMJA: 2021) 68

M. Tokson, "The Aftermath of *Carpenter*: An Empirical Study of Fourth Amendment Case Law, 2018-2021," 135 Harvard L. Rev. ___ (2021) (forthcoming) 68

A.Vittorio, "Robbery Poses Legal Test for Police Use of Google Location Data," *Bloomberg Law News* (Sept. 14, 2021) 69

D.C. Weiss, "Judge Permits Prosecutors to Use Facial Recognition to Open Accused Capitol Rioter's Laptop," *ABA J. Daily News* (July 23, 2021) 69

Z. Whittaker, "Google Says Geofence Warrants Make Up One-Quarter of All US Demands," *TechCrunch* (Aug. 19, 2021) 69

FOREWARD TO THE APRIL 2022 EDITION

The first edition of *Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials* was published in February 2016. That edition attempted to be a comprehensive collection of case law and materials that provided guidance on how electronic information featured in criminal investigations and proceedings. Later supplements followed the first edition and, in December of 2017, a new edition was published that incorporated everything into a single compilation. Thereafter, in September 2019, August 2020, and April 2021, editions were published that updated the compilation. The time has come to publish yet another supplement.

This latest supplement features links to materials, as does its predecessor. The links were last visited when it was completed in April 2022. The reader is cautioned that specific links may have become stale over time.

Now, a personal note: I began this undertaking with the intent of selecting a handful of decisions to illustrate how electronic information has impacted criminal law and procedure. Why? We live at a time when electronic information is "everywhere" and comes in many shapes and sizes or, put in other words, ever-increasing volumes, varieties, and velocities. As with every other product of the human imagination, electronic information can be used for good or bad. Those uses raise many issues in the context of criminal investigations and proceedings and electronic information is now a common feature in the commission, investigation, and prosecution of crimes. Among other things, those issues present questions of how the Bill of Rights and equivalent State constitutional guarantees apply to electronic information. Moreover, new sources of electronic information and technologies appear on a seemingly daily basis and must be "fitted" into constitutional and statutory frameworks. I hope that this new supplement, along with its predecessors, will inform the groups of actors in the criminal justice system, whether judicial, law enforcement, prosecution, defense, or support, on how issues arising out of electronic information might be presented and resolved.

Every edition has been posted on the website of the Massachusetts Attorney General's Office. I want to thank Attorney General Healey for allowing the postings. I also want to others in that office, as well as Tom Ralph, for making the postings possible.

TAGS

#Admissibility

#CSLI

#Discovery Materials

#Encryption

#Fifth Amendment – Self-Incrimination

#Fourth Amendment – Ex Ante Conditions

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#International

#Miscellaneous

#Preservation and Spoliation

#Probation and Supervised Release

#Reasonable Expectation of Privacy

#Sixth Amendment – Assistance of Counsel

#Sixth Amendment – Right of Confrontation

#SCA (Stored Communications Act)

#Social Media

#Third-Party Doctrine

#Trial-Related

ABBREVIATIONS

"Cell Site Location Information" – CSLI

"Stored Communications Act" – SCA

DECISIONS – UNITED STATES SUPREME COURT

Andrews v. State, No. 20-937, *cert.* denied (U.S. May 17, 2021), decision below, *State v. Andrews*, 243 N.J. 447 (2020)

#Fifth Amendment – Self-Incrimination

Caniglia v. Strom, No. 20-157, 2021 WL 1951784 (U.S. May 17, 2021)

The petitioner commenced a Section 1983 action against the respondent police officers, who entered his home and seized him and his weapons without a warrant. The Court of Appeals affirmed the entry of summary judgment in favor of the officers, concluding that their actions fell within a "community caretaking exception" to the Warrant Requirement. The Supreme Court reversed in a unanimous decision:

> To be sure, the Fourth Amendment does not prohibit all unwelcome intrusions "on private property," *ibid*.—only "unreasonable" ones. We have thus recognized a few permissible invasions of the home and its curtilage. Perhaps most familiar, for example, are searches and seizures pursuant to a valid warrant. See *Collins v. Virginia*, 584 U.S. ___, ___-___ (2018) (slip op., at 5-6). We have also held that law enforcement officers may enter private property without a warrant when certain exigent circumstances exist, including the need to "'render emergency assistance to an injured occupant or to protect an occupant from imminent injury.'" *Kentucky v. King*, 563 U. S. 452, 460, 470 (2011); see also *Brigham City v. Stuart*, 547 U. S. 398, 403–404 (2006) (listing other examples of exigent circumstances). And, of course, officers may generally take actions that "'any private citizen might do'" without fear of liability. *E.g., Jardines,* 569 U. S., at 8 (approaching a home and knocking on the front door).
>
> The First Circuit's "community caretaking" rule, however, goes beyond anything this Court has recognized. The decision below assumed that respondents lacked a warrant or consent, and it expressly disclaimed the possibility that they were reacting to a crime. The court also declined to consider whether any recognized exigent circumstances were present because respondents had forfeited the point. Nor did it find that respondents' actions were akin to what a private citizen might have had authority to do if petitioner's wife had approached a neighbor for assistance instead of the police. Neither the holding nor logic of *Cady* justified that approach. True, *Cady* also involved a warrantless search for a firearm. But the location of that search was an impounded vehicle—not

> a home—"'a constitutional difference'" that the opinion repeatedly stressed. 413 U. S., at 439; see also *id.*, at 440–442. In fact, *Cady* expressly contrasted its treatment of a vehicle already under police control with a search of a car "parked adjacent to the dwelling place of the owner." *Id.*, at 446–448 (citing *Coolidge v. New Hampshire*, 403 U. S. 443 (1971)).
>
> *Cady*'s unmistakable distinction between vehicles and homes also places into proper context its reference to "community caretaking." This quote comes from a portion of the opinion explaining that the "frequency with which . . . vehicle[s] can become disabled or involved in . . . accident[s] on public highways" often requires police to perform noncriminal "community caretaking functions," such as providing aid to motorists. 413 U. S., at 441. But, this recognition that police officers perform many civic tasks in modern society was just that—a recognition that these tasks exist, and not an open-ended license to perform them anywhere.
>
> ***
>
> What is reasonable for vehicles is different from what is reasonable for homes. *Cady* acknowledged as much, and this Court has repeatedly "declined to expand the scope of . . . exceptions to the warrant requirement to permit warrantless entry into the home." *Collins*, 584 U. S., at ___ (slip op., at 8). We thus vacate the judgment below and remand for further proceedings consistent with this opinion.

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

City of Tahlequah v. Bond, No. 20-1668, 2021 WL 4822664 (U.S. Oct. 18, 2021) (*per curiam*)

The police officer defendants in this Section 1983 action were sued for violating a decedent's Fourth Amendment right to be free from excessive force. The officers had shot the decedent after he advanced on them with a hammer. The district court granted summary judgment in the officers' favor on the merits and on qualified immunity grounds. The Tenth Circuit reversed, concluding that there was a disputed question of fact whether the officers had recklessly created the situation that led to the shooting. The Supreme Court reversed:

> We need not, and do not, decide whether the officers violated the Fourth Amendment in the first place, or whether recklessly creating a situation that requires deadly force can itself violate the Fourth Amendment. On

this record, the officers plainly did not violate any clearly established law.

The doctrine of qualified immunity shields officers from civil liability so long as their conduct 'does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.' *Pearson v. Callahan*, 555 U. S. 223, 231 (2009). As we have explained, qualified immunity protects 'all but the plainly incompetent or those who knowingly violate the law.' *District of Columbia v. Wesby*, 583 U. S. ___, ___ –___ (2018) (slip op., at 13–14) (quoting *Malley v. Briggs*, 475 U. S. 335, 341 (1986)).

We have repeatedly told courts not to define clearly established law at too high a level of generality. See, *e.g., Ashcroft v. al-Kidd*, 563 U. S. 731, 742 (2011). It is not enough that a rule be suggested by then-existing precedent; the 'rule's contours must be so well defined that it is 'clear to a reasonable officer that his conduct was unlawful in the situation he confronted.'' *Wesby*, 583 U. S., at ___ (slip op., at 14) (quoting *Saucier v. Katz*, 533 U. S. 194, 202 (2001)). Such specificity is 'especially important in the Fourth Amendment context,' where it is 'sometimes difficult for an officer to determine how the relevant legal doctrine, here excessive force, will apply to the factual situation the officer confronts.' *Mullenix v. Luna*, 577 U. S. 7, 12 (2015) (*per curiam*) (internal quotation marks omitted).

The Tenth Circuit contravened those settled principles here. Not one of the decisions relied upon by the Court of Appeals—*Estate of Ceballos v. Husk*, 919 F. 3d 1204 (CA10 2019), *Hastings v. Barnes*, 252 Fed. Appx. 197 (CA10 2007), *Allen*, 119 F. 3d 837, and *Sevier v. Lawrence*, 60 F. 3d 695 (CA10 1995)—comes close to establishing that the officers' conduct was unlawful. The Court relied most heavily on *Allen*. But the facts of *Allen* are dramatically different from the facts here. The officers in *Allen* responded to a potential suicide call by sprinting toward a parked car, screaming at the suspect, and attempting to physically wrest a gun from his hands. 119 F. 3d, at 841. Officers Girdner and Vick, by contrast, engaged in a conversation with Rollice, followed him into a garage at a distance of 6 to 10 feet, and did not yell until after he picked up a hammer. We cannot conclude that *Allen* 'clearly established' that their conduct was reckless or that their ultimate use of force was unlawful.

***

Neither the panel majority nor the respondent have identified a single precedent finding a Fourth Amendment violation under similar circumstances. The officers were thus entitled to qualified immunity.

#Fourth Amendment – Good Faith Exception

Lange v. California, No. 20-18, 2021 WL 2557068 (U.S. June 23, 2021)

> The Fourth Amendment ordinarily requires that police officers get a warrant before entering a home without permission. But an officer may make a warrantless entry when 'the exigencies of the situation' create a compelling law enforcement need. *Kentucky v. King*, 563 U. S. 452, 460 (2011). The question presented here is whether the pursuit of a fleeing misdemeanor suspect always—or more legally put, categorically—qualifies as an exigent circumstance. We hold it does not. A great many misdemeanor pursuits involve exigencies allowing warrantless entry. But whether a given one does so turns on the particular facts of the case. ***
>
> The flight of a suspected misdemeanant does not always justify a warrantless entry into a home. An officer must consider all the circumstances in a pursuit case to determine whether there is a law enforcement emergency. On many occasions, the officer will have good reason to enter—to prevent imminent harms of violence, destruction of evidence, or escape from the home. But when the officer has time to get a warrant, he must do so—even though the misdemeanant fled.
>
> Because the California Court of Appeal applied the categorical rule we reject today, we vacate its judgment and remand the case for further proceedings not inconsistent with this opinion.

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

Merchant v. Mayorkas, No. 20-1505, *cert.* denied, 2021 WL 2637881 (U.S. June 28, 2021), decision below, *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021)

#Fourth Amendment – Warrant Required or Not

Rivas-Villegas v. Cortesluna, No. 20-1539, 2021 WL 4822662 (U.S. Oct. 18, 2021) (*per curiam*)

This was a Section 1983 action brought against the petitioner police officer for excessive use of force by placing his knee on the respondent's back while removing a knife the respondent was carrying and handcuffing him. The Court of Appeals held that the officer was not entitled to qualified immunity based on existing Ninth Circuit precedent. The Supreme Court reversed:

'Qualified immunity attaches when an official's conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.' *White v. Pauly*, 580 U. S. ___, ___ (2017) (*per curiam*) (slip op., at 6) (internal quotation marks omitted). A right is clearly established when it is 'sufficiently clear that every reasonable official would have understood that what he is doing violates that right.' *Mullenix v. Luna*, 577 U. S. 7, 11 (2015) (*per curiam*) (internal quotation marks omitted). Although 'this Court's case law does not require a case directly on point for a right to be clearly established, existing precedent must have placed the statutory or constitutional question beyond debate.' *White*, 580 U. S., at ___ (slip op., at 6) (alterations and internal quotation marks omitted). This inquiry 'must be undertaken in light of the specific context of the case, not as a broad general proposition.' *Brosseau v. Haugen*, 543 U. S. 194, 198 (2004) (*per curiam*) (internal quotation marks omitted).

'[S]pecificity is especially important in the Fourth Amendment context, where . . . it is sometimes difficult for an officer to determine how the relevant legal doctrine, here excessive force, will apply to the factual situation the officer confronts.' *Mullenix*, 577 U. S., at 12 (alterations and internal quotation marks omitted). Whether an officer has used excessive force depends on "the facts and circumstances of each particular case, including the severity of the crime at issue, whether the suspect poses an immediate threat to the safety of the officers or others, and whether he is actively resisting arrest or attempting to evade arrest by flight." *Graham v. Connor*, 490 U. S. 386, 396 (1989); see also *Tennessee v. Garner*, 471 U. S. 1, 11 (1985) ('Where the officer has probable cause to believe that the suspect poses a threat of serious physical harm, either to the officer or to others, it is not constitutionally unreasonable to prevent escape by using deadly force'). However, *Graham*'s and *Garner*'s standards are cast 'at a high level of generality.' *Brosseau*, 543 U. S., at 199. '[I]n an obvious case, these standards can 'clearly establish' the answer, even without a body of relevant case law.' *Ibid*. But this is not an obvious case. Thus, to show a violation of clearly established law, Cortesluna must identify a case that put Rivas-Villegas on notice that his specific conduct was unlawful.

Cortesluna has not done so. Neither Cortesluna nor the Court of Appeals identified any Supreme Court case that addresses facts like the ones at issue here. Instead, the Court of Appeals relied solely on its precedent in *LaLonde*. Even assuming that Circuit precedent can clearly establish law for purposes of §1983, *LaLonde* is materially distinguishable and thus does not govern the facts of this case.

In *LaLonde*, officers were responding to a neighbor's complaint that LaLonde had been making too much noise in his apartment. 204 F. 3d, at 950–951. When they knocked on LaLonde's door, he 'appeared in his underwear and a T-shirt, holding a sandwich in his hand.' *Id.*, at 951. LaLonde testified that, after he refused to let the officers enter his home, they did so anyway and informed him he would be arrested for obstruction of justice. *Ibid*. One officer then knocked the sandwich from LaLonde's hand and 'grabbed LaLonde by his ponytail and knocked him backwards to the ground.' *Id.*, at 952. After a short scuffle, the officer sprayed LaLonde in the face with pepper spray. At that point, LaLonde ceased resisting and another officer, while handcuffing LaLonde, 'deliberately dug his knee into LaLonde's back with a force that caused him long-term if not permanent back injury.' *Id.*, at 952, 960, n. 17.

The situation in *LaLonde* and the situation at issue here diverge in several respects. In *LaLonde*, officers were responding to a mere noise complaint, whereas here they were responding to a serious alleged incident of domestic violence possibly involving a chainsaw. In addition, LaLonde was unarmed. Cortesluna, in contrast, had a knife protruding from his left pocket for which he had just previously appeared to reach. Further, in this case, video evidence shows, and Cortesluna does not dispute, that Rivas-Villegas placed his knee on Cortesluna for no more than eight seconds and only on the side of his back near the knife that officers were in the process of retrieving. LaLonde, in contrast, testified that the officer deliberately dug his knee into his back when he had no weapon and had made no threat when approached by police. These facts, considered together in the context of this particular arrest, materially distinguish this case from *LaLonde*.

'Precedent involving similar facts can help move a case beyond the otherwise hazy borders between excessive and acceptable force and thereby provide an officer notice that a specific use of force is unlawful.' *Kisela v. Hughes*, 584 U. S. ___, ___ (2018) (*per curiam*) (slip op., at 5) (internal quotation marks omitted). On the facts of this case, neither *LaLonde* nor any decision of this Court is sufficiently similar. For that reason, we grant Rivas-Villegas' petition for certiorari and reverse the Ninth Circuit's determination that Rivas-Villegas is not entitled to qualified immunity.

#Fourth Amendment – Good Faith Exception

Van Buren v. United States, No. 19-783, 2021 WL 2229206 (U.S. June 3, 2021)

The defendant, a former Georgia police sergeant, used his patrol car computer to access a law enforcement database for information about a license plate number in exchange for money. He was prosecuted as part of a FBI sting operation and convicted under the Computer Fraud and Abuse Act, which makes it illegal "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Interpreting the CFAA, the Court, in a majority opinion authored by Justice Barrett, held that the defendant had not violated the statute. The provision in issue "covers those who obtain information from particular areas in the computer – such as files, folders, or databases – to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them."

#Miscellaneous

DECISIONS – FEDERAL

In re Capitol Breach Grand Jury Investigations Within the District of Columbia, Grand Jury Action No. 21-20 (BAH), 2021 WL 3021465 (D.D.C. July 16, 2021)

This was an application by the Government for an order that would authorize disclosure of "massive amounts of information and electronic data" secured in its investigation of the January 6th Insurrection to an independent contactor, Deloitte Financial Advisory Services, LLP, "to assist in document processing, review, and production." Certain of these materials were presented to a grand jury and the Government sought to disclose to Deloitte "grand jury matters related to the Capitol attack and materials collected in connection with those matters." The court denied the Government's application, concluding that "Deloitte and its employees are not 'government personnel' within the meaning of Rule 6(e)(3)(A)(ii) and the government has not made the requisite showing of particularized need for an order authorizing disclosure under Rule 6(e)(3)(E)(i)."

#Discovery Materials

#Miscellaneous

Harbor Healthcare System, L.P. v. United States, No. 19-20624, 2021 WL 3009732 (5th Cir. July 15, 2021) (*per curiam*)

This was an appeal from an order by the district court below that denied the plaintiff's pre-indictment motion under *Fed. R. Crim. P.* 41(g) for the return of documents seized in searches of the plaintiff's locations and offices. The plaintiff was the subject of two *qui tam* actions and federal prosecutors secured warrrants for the searches. The plaintiff sought the return of materials allegedly subject to the attorney-client privilege and, after an agreement could not be reached with the Government, commenced a civil action for their return. The district court declined to exercise its equitable jurisdiction and dismissed the action, concluding that the Government had an adequate screening process in place and the plaintiff could seek post-indictment relief. The Court of Appeals reversed. First, the dismissal of the motion was a final, appealable decision and the Government "cannot ever say" whether a grand jury proceeding existed. On the merits, the appellate court found that the district court had abused its discretion by failing to exercise its equitable jurisdiction:

> The government's ongoing intrusion on Harbor's privacy constitutes an irreparable injury that can be cured only by Rule 41(g) relief. Harbor remains injured as long as the government retains its privileged documents. That injury can only be made whole by the government returning and destroying its copies of the privileged material. ***
>
> Finally, Harbor does not have an adequate remedy at law. A motion to suppress in a possible criminal proceeding does not redress Harbor's injury for two primary reasons. First, it is not certain that there ever will be criminal charges brought against Harbor. If no charges are brought but a suppression motion is Harbor's only means of redress, Harbor would never have an opportunity to challenge the government's seizure of its privileged materials. Second, suppression motions vindicate an interest entirely different from Rule 41(g) motions. Suppression merely prevents the government from using certain materials as evidence in a judicial proceeding—suppression does not force the government to return those materials to the criminal defendant. *** Rule 41(g), by contrast, says nothing about the admissibility of evidence. Instead, it is concerned solely with the return of property to the Rule 41(g) movant. Suppression and Rule 41(g) occupy two entirely distinct spheres within the universe of unlawful searches and seizures.
>
> The government unconvincingly argues that suppression is an adequate remedy because Rule 41(g), like suppression, is concerned with unlawful

> searches and seizures. That argument overlooks the distinction explained above. Suppression protects criminal defendants from the procedural harm arising from the introduction of unlawfully seized evidence. Rule 41(g) protects persons from the 'deprivation of property' by an unlawful search and seizure. It makes little sense to say that the Fourth Amendment can be litigated only in a suppression motion when there are other types of harm arising from unlawful searches and seizures. This is particularly true since Rule 41(g) expressly contemplates such a harm and offers a remedy.
>
> In short, the district court erred by misunderstanding the harm alleged by Harbor and by equating return of property with suppression of evidence. It therefore abused its discretion by refusing jurisdiction over Harbor's Rule 41(g) motion. [footnotes omitted].

The Court of Appeals also considered how the documents in issue might be reviewed by the court below:

> The district court expressed concern about the practicality of it parsing through reams of Harbor documents to rule on claims of privilege. The district court's concern can be assuaged by the array of document-review options. For starters, the government could simply be ordered to return the documents for which it does not dispute the asserted basis for the privilege. For the balance, the court could engage a magistrate judge or special master to review the potentially privileged documents. Even this will not entail reviewing each and every document; Harbor's privilege logs should allow for recommendations or rulings based on categories of documents. ***

#Discovery Materials

#Miscellaneous

Mexican Gulf Fishing Co. v. U.S. Dep't of Commerce, Civil Action No. 20-2312, 2022 WL 594911 (E.D. La. Feb. 28, 2022)

This was a challenge by a group of charter board captains and boat owners to a Final Rule published by the federal defendants that, among other things, imposed a tracking requirement on regulated vessels. The district court assumed without deciding that the requirement was a search for Fourth Amendment purposes but that it was reasonable under the "closely regulated industry" exception to the Warrant Requirement because (1) the fishing industry is a closely regulated one "because of the long history of regulation meant to protect a valuable resource and,

subsequently, the public," and (2) the requirement satisfied the three criteria established by *New York v. Burger*, 482 U.S. 691 (1987).

#Fourth Amendment – Warrant Required or Not

Project Veritas Action Fund v. Rollins, Nos. 19-1586, 19-1640, 2020 WL 7350243 (1st Cir. Dec. 15, 2020), *cert.* denied, No. 20-1598, 2021 WL 5434360 (U.S. Nov. 22, 2021)

> Massachusetts, like other states concerned about the threat to privacy that commercially available electronic eavesdropping devices pose, makes it a crime to record another person's words secretly and without consent. But, unlike other concerned states, Massachusetts does not recognize any exceptions based on whether that person has an expectation of privacy in what is recorded. See Mass. Gen. Laws ch. 272, § 99 ("Section 99"). As a result, Massachusetts makes it as much a crime for a civic-minded observer to use a smartphone to record from a safe distance what is said during a police officer's mistreatment of a civilian in a city park as it is for a revenge seeker to hide a tape recorder under the table at a private home to capture a conversation with an ex-spouse. The categorical and sweeping nature of Section 99 gives rise to the important questions under the First Amendment to the United States Constitution that the challenges that underlie the consolidated appeals before us present.
>
> The first appeal that we address stems from a 2016 suit filed in the District of Massachusetts by two civil rights activists in Boston -- K. Eric Martin and René Pérez ('the Martin Plaintiffs'). They allege that Section 99 violates the First Amendment insofar as it criminalizes the secret, nonconsensual audio recording of police officers discharging their official duties in public spaces. The other appeal that we address stems from a suit filed in that same year in that same district -- and eventually resolved by the same district court judge -- by Project Veritas Action Fund ('Project Veritas'), which is a national media organization dedicated to 'undercover investigative journalism.'
>
> Project Veritas's suit targets Section 99 insofar as it bans the secret, nonconsensual audio recording of any government official discharging official duties in public spaces, as well as insofar as it bans such recording of any person who does not have a reasonable expectation of privacy in what is recorded. Project Veritas also alleges that Section 99 must be struck down in its entirety pursuant to the First Amendment doctrine of overbreadth.

We affirm the District Court's grant of summary judgment to the Martin Plaintiffs, based on its ruling that Section 99 violates the First Amendment by prohibiting the secret, nonconsensual audio recording of police officers discharging their official duties in public spaces. We also affirm the District Court's order dismissing Project Veritas's First Amendment overbreadth challenge for failing to state a claim on which relief may be granted. However, we vacate on ripeness grounds the District Court's order dismissing with prejudice Project Veritas's First Amendment challenge to Section 99 insofar as that statute prohibits the secret, nonconsensual audio recording of individuals who lack an expectation of privacy in what is recorded. For the same reason, we vacate the District Court's grant of summary judgment to Project Veritas on its claim that Section 99 violates the First Amendment insofar as that statute bars the secret, nonconsensual audio recording of government officials discharging their duties in public. We remand the claims asserting these two latter challenges to the District Court with instructions to dismiss them without prejudice for lack of subject matter jurisdiction. ***

The privacy that we enjoy, even in public, is too important to be taken for granted. Cf. Carpenter v. United States, 138 S. Ct. 2206, 2217-18 (2018) (first citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in judgment), then citing id. at 415 (Sotomayor, J., concurring)). But, so, too, is the role that laypersons can play in informing the public about the way public officials, and law enforcement in particular, carry out their official duties.

We conclude that, by holding that Section 99 violates the First Amendment in criminalizing the secret, nonconsensual audio recording of police officers discharging their official duties in public spaces and by granting declaratory relief to the Martin Plaintiffs, the District Court properly accounted for the values of both privacy and accountability within our constitutional system. We further conclude that the District Court properly rejected Project Veritas's First Amendment overbreadth challenge, in which the organization sought to invalidate the measure in its entirety, given the substantial protection for privacy that it provides in contexts far removed from those that concern the need to hold public officials accountable. Finally, we vacate and remand the District Court's rulings as to the remainder of Project Veritas's challenges, because, in their present state, they ask us to engage in an inquiry into sensitive and difficult First Amendment issues -- concerning both privacy in public and government accountability -- that is too likely to be a hypothetical one, given the disconnect between the organization's concrete allegations regarding its intentions and the breadth of the relief it seeks.

> We thus affirm the District Court's judgment in the Martin Plaintiffs' case and affirm in part and vacate and remand in part its judgment in Project Veritas's. The parties shall bear their own costs.

#Miscellaneous

#Reasonable Expectation of Privacy

I/M/O Search of Information That Is Stored at the Premises Controlled by Google LLC, Case No. 21-SC-3217 (GMH), 2021 WL 6196136 (D.D.C. Dec. 30, 2021)

The Government applied for a warrant. As described by the Court:

> It is what has been termed a 'reverse-location' warrant: the perpetrator of the crime being unknown to law enforcement, the warrant identifies the geographic location where criminal activity happened and seeks to identify cell phone users at that location when the crime occurred. The 'geofence' is the boundary of the area where the criminal activity occurred, and is drawn by the government using geolocation coordinates on a map attached to the warrant. [footnote omitted].

The application for the warrant sought data for a total of 185 minutes split into segments over a five and a half month period that corresponded to the criminal activity under investigation. After the Government proposed a protocol to obtain the data from Google and the Magistrate Judge expressed concerns about the process that had been proposed, the Government submitted a revised protocol which he approved:

> a. Using Location History data, Google will identify those devices that it calculated were within the [geofence area] during the course of the time periods laid forth in [the warrant].
>
> b. For each device: Google will provide an anonymized identifier that Google creates and assigns to device for purposes of responding to this search warrant; Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (i.e., 'maps display radius'), and source(s) from which the location data was derived (e.g., GPS, Wi-Fi, Bluetooth), if available. Google will not, in this step, provide the Google account identifiers (e.g., example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.
>
> c. The government will then review this list to identify devices, if any, that it can determine are not likely to be relevant to the investigation (for

> example, devices moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case).
>
> d. *The government must then, in additional legal process to the Court,* identify the devices appearing on the list produced by Google for which the government seeks the Google account identifier and basic subscriber information.
>
> e. In response to this additional legal process, *the Court may then order Google* to disclose to the government the Google account identifier associated with the devices identified by the government to the Court, along with basic subscriber information for those accounts.

The revised protocol gave the court "the discretion as to what devices falling within the geofence to deanonymize," rather than the Government (as had the original proposal).

The Magistrate Judge found that probable cause had been shown:

> Thus, because there is a 'fair probability' that (i) the suspects were inside the geofence, (ii) were using their cell phones inside the geofence, (iii) those phones communicated location information to Google, and (iv) Google can trace that information back to a particular device, accountholder, and/or subscriber, there is probable cause that the search will produce evidence useful to the government's investigation of the criminal activity in question.

He also found that particularity had been established:

> Finally, the government has satisfied the particularity requirement as to the place to be searched because, as discussed below, it has appropriately contoured the temporal and geographic windows in which it is seeking location data. That is, the government has limited the place to be searched in time and location, and its warrant application is not otherwise overly-broad, but is 'confined to the breadth of the probable cause that supports it.' [citations omitted].

The court also found that the warrant would not be overbroad given the time periods during which data would be collected and the geographic contours of the geofence, which encompassed an industrial rather than a residential area. Overbreadth concerns were also met by the protocol, which ensured that "identifying information associated with devices will be produced only pursuant to a further directive from the Court."

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

I/M/O Search of Information that is Stored at the Premises Controlled by Google, LLC, Case No. 21-MJ-5064-ADM, 2021 WL 2401925 (D. Kan. June 4, 2021)

The Government applied for a geofence warrant for "location history data covering a defined area that surrrounds and includes a building where a federal crime allegedly occurred." The application sought data for a one-hour period. The magistrate judge denied the application without prejudice because it failed to meet the Probable Cause and Particularity Requirements: (1) the agent's statements in the application were "too vague and generic to establish a fair probability—or any probability—that the identity of the perpretrator or witnesses would be encompassed within the search," (2) the statements did not "establish a fair probability that any pertinent individual would have been using a device that feeds into Google's location-tracking technology," and (3) the application did not address the "anticipated number of individuals likely to be encompassed within the targeted Google location data." The judge also found that the application was deficient because the warrant could return data from users who were outside the geofence and there was no "reasonable explanation" for the time period sought.

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

In re Search Warrants Executed on Apr. 28, 2021, 21-MC-425 (JPO), 2021 WL 2188150 (S.D.N.Y. May 28, 2021)

This matter arose out of warrants to search premises and electronic devices belonging to, among others, Rudolph Giuliani. Giuliani and another individual sought certain relief, all of which the issuing magistrate judge denied. First, the judge denied their request for return of the materials which, in effect, would have required the Government to proceed by subpoena as there was no legal support for that position. Next, the judge rejected the argument that their status as lawyers made the searches "problematic" because (1) lawyers are not immune from searches in criminal investigations, and (2) the searches were based on probable cause. The judge also found that a filter team process established as to earlier search warrants was adequate and that the individuals were not entitled to pre-indictment discovery of any "privilege and responsiveness" designations made by the Government with regard to materials seized pursuant to those warrants. The court then denied Giuliani's request that the affidavits in support of all the warrants

be unsealed, finding that the need to protect grand jury secrecy trumped any right of access. The court also granted the Government's request to appoint a special master to conduct a filter review of documents seized pursuant to the new warrants.

#Discovery Materials

#Miscellaneous

United States v. Bebris, No. 20-3291, 2021 WL 2979520 (7th Cir. July 15, 2021)

The defendant sent child pornography over Facebook's private user-to-user system, Facebook Messenger. His conduct was discovered by Facebook, which used image-recognition technology developed by Microsoft called PhotoDNA to compare images in three of the defendant's messages against a database of known child pornography. As required by law, Facebook reported the images to the National Center for Missing and Exploited Children ("NCMEC"), which in turn reported the images to Wisconsin law enforcement officers, who secured a search warrant and found a computer containing child pornography. The defendant was charged under federal law with possessing and distributing child pornography. He moved to suppress the evidence, arguing that Facebook acted as a government agent by monitoring its platform and reporting the defendant. After the district court denied the motion, the defendant pled guilty to one count of distribution, reserving his right to appeal the denial of his motion to suppress. On appeal, the defendant argued that the district court deprived him of the opportunity to prove Facebook's role by denying his request for a *Fed. R. Crim. P*. 17(a) subpoena seeking pre-trial testimony of a Facebook employee:

> As a general, initial matter, Bebris's challenge to Facebook's search of his messages and his assertion that this search violated the Fourth Amendment draws from an argument that has become familiar to federal district and circuit courts around the country. Bebris's core theory is that Facebook's use of the PhotoDNA technology, along with other facts he presented or hoped to present (if they existed), converted Facebook into a government agent for Fourth Amendment purposes. Thus, Bebris contends that the evidence recovered and transferred as a result of Facebook's search should have been suppressed because it was obtained without a warrant. This theory is not novel and has been invoked in various circumstances involving PhotoDNA or similar technology. ***
>
> Bebris, however, has added a twist to this common argument. He asserts that he has been deprived of the opportunity to prove that Facebook

> acted as a government agent because the district court quashed his subpoena for live testimony from a Facebook representative at the evidentiary hearing on Bebris's motion to suppress. The district court's quashing of the subpoena, he argues, constituted a violation of the Confrontation Clause of the Sixth Amendment. In other words, Bebris argues that the ultimate denial of his motion to suppress (in which he claimed Fourth Amendment violations) was predicated on the district court's refusal to require testimony from a Facebook representative (which, as he sees it, violated his Sixth Amendment Confrontation Clause right). Bebris additionally argues that even if the district court did not err by quashing the Facebook subpoena, the district court still erred by denying the motion to suppress on the merits based on the evidence in the record. Bebris also argues that the district court erred by finding that he lacked a reasonable expectation of privacy in his Facebook messages. We address each argument in turn below.

The Court of Appeals affirmed. The district court did not err in its finding that Facebook was a private actor and the search was not later expanded, the Confrontation Clause was inapplicable at the suppression hearing, and the district court did not err in quashing the subpoena because additional testimony would have been merely cumulative to evidence in the record. The Seventh Circuit did not reach the question whether the defendant had a reasonable expectation of privacy in his messages or whether the good faith exception to the Warrant Requirement might be applicable.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Sixth Amendment – Right of Confrontation

United States v. Caesar, No. 19-3961, 2021 WL 2559471 (3d Cir. June 23, 2021)

> Facing federal child pornography charges, defendant appellee Robert Caesar moved to suppress evidence seized pursuant to search warrants executed by the Pennsylvania State Police. The District Court granted the motion in part, suppressing thousands of images of child pornography and photographs of Caesar's sexual abuse victims. The Government now appeals.
>
> The initial warrant application contained information that Caesar had sexually abused two children in his home and, on multiple occasions, took to the Internet seeking out used children's undergarments and photos and videos of partially clothed children. Although the supporting

> affidavit included no express allegations that Caesar possessed child pornography, it stated that child abusers 'routinely keep' such images. App. 49. The magistrate judge issued a warrant authorizing officers to search Caesar's home for child pornography and other sexually explicit images of minors, among other things, and several items of electronic equipment, later found to contain child pornography, were seized. Charged under federal law with producing, receiving, and possessing child pornography, Caesar moved to suppress the images. The District Court excluded the images, determining that the statements linking child molestation with child pornography failed to establish probable cause. It further concluded that the affidavit was so deficient that the good faith exception to the exclusionary rule did not apply. Because we conclude that the officers relied on the initial warrant in good faith, we will reverse that part of the District Court order suppressing the images and remand for further proceedings.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Chatrie, Criminal Case No. 3:19cr130, 2022 WL 628905 (E.D. Va. Mar. 3, 2022)

The Government secured a warrant for geofence information that tied the defendant to the vicinity of a bank robbery. After he was charged with two crimes related to the robbery, the defendant moved to suppress evidence derived from the warrant. The court conducted hearings on the motion, heard testimony from experts for the Government and the defendant, and had the benefit of multiple rounds of briefing. In its decision, the court discussed Google's location services as well as its "typical response to geofence warrants." The court found that the warrant application failed to show probable cause but that the good faith exception to the Warrant Requirement applied.

#CSLI

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

United States v. Dennis, 20 Cr. 623 (LGS) (S.D.N.Y. Jan. 26, 2022)

The defendant sought modification of the conditions of his pretrial release. The district court denied the application:

> Defendant seeks a modification of his conditions of pretrial release based on two sets of purported new facts: (1) Defendant has complied with his release conditions and (2) Defendant has experienced 'significant physical pain and injury' as a result of his location monitoring equipment. Since Defendant initially submitted his letter, he has provided an additional record that states his current medical provider, a physician, explained to him 'that the bracelet on his right ankle is unlikely to be the cause of the right inguinal hernia.' His prior provider, a physician assistant-certified, reached a conflicting conclusion. The Court accords the physician's evaluation more weight because it is more recent and it is from a physician rather than a physician assistant. Based on the physician's evaluation, this Court has no basis to find that Defendant is experiencing physical pain and injury as a result of his location monitoring equipment at this time. That leaves Defendant's other 'new' evidence, that the conditions of his bail have been effective. This evidence is new in that it could not have been presented when those conditions were imposed but the evidence is not unexpected -- when the conditions were set, they were set with the expectation that Defendant would comply. Nothing in Defendant's letters changes the analysis of the factors enumerated in 18 U.S.C. § 3142(g), which guide review of an application to modify a defendant's bail conditions. So there is no basis for a modification or hearing.

#Probation and Supervised Release

United States v. Fleury, No. 20-11037, 2021 WL 5933789 (11th Cir. Dec. 16, 2021)

The defendant was convicted of transmitting interstate threats and cyberstalking. The convictions stemmed from posts he made and Instagram messages in which he posed as various mass murderers. These were directed to three individuals who lost loved ones in a school shooting in Florida. On appeal, he challenged the sufficiency of the indictment and evidence, the jury instructions, and the admission of expert testimony. The Court of Appeals affirmed. It rejected the defendant's argument that the cyberstalking statute was facially unconstitutional:

> Fleury has not met his burden of demonstrating that § 2261A(2)(B) is unconstitutionally overbroad. His facial challenge fails because it ignores

> key statutory elements that narrow the conduct it applies to—including, for example, proof that the defendant acted with 'intent to kill, injure, harass, [or] intimidate' and evidence that the defendant 'engage[d] in a course of conduct' consisting of two or more acts evidencing a continuity of purpose. 18 U.S.C. § 2261A(2)(B). Further, '[t]he mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge.' *Williams*, 553 U.S. at 303 (internal quotation marks omitted). The Supreme Court has 'vigorously enforced the requirement that a statute's overbreadth be substantial, not only in an absolute sense, but also relative to the statute's plainly legitimate sweep.' *Id*. at 292–93.
>
> Because § 2261A(2)(B) is not 'substantial[ly]' overbroad, we uphold the constitutionality of the statute. *See id*. In doing so we join every circuit court of appeals that has addressed a facial attack to § 2261A(2)(B). *See United States v. Ackell*, 907 F.3d 67, 73 (1st Cir. 2018) (concluding that § 2261A(2)(B) does not target speech, and therefore is not unconstitutionally overbroad, because even though the statute 'could reach highly expressive conduct, it is plain from the statute's text that it covers countless amounts of unprotected conduct'); *United States v. Petrovic*, 701 F.3d 849, 856 (8th Cir. 2012) (concluding, under the prior version of the statute, that '[m]ost, if not all, of the statute's legal applications are to conduct that is not protected by the First Amendment' (alteration adopted)); *United States v. Osinger*, 753 F.3d 939, 944 (9th Cir. 2014) (rejecting an overbreadth challenge to the prior version of § 2261A(2)(B) and concluding that because the statute 'proscribes harassing and intimidating conduct, the statute is not facially invalid').

The Eleventh Circuit also rejected the defendant's as-applied challenge:

> Fleury's as-applied challenge fares no better than his facial challenge. While it's feasible to think of limited instances in which § 2261A(2)(B) could apply to constitutionally-protected speech, Fleury's case is not one of them. He argues that the statute is unconstitutional as applied to his conduct because (1) his speech concerned a matter of public concern, and (2) the statute impermissibly restricts the content of his speech. Neither argument has merit.
>
> ***
>
> When viewing Fleury's messages within the context of his entire course of conduct—including the sheer number and frequency of the messages—they create the visual of an anonymous, persistent tormenter who desires to harm the victims. This is precisely the type of fear that the 'true threats' doctrine is intended to prevent. *See Black*, 538 U.S. at 360

> (noting that a prohibition on true threats serves to protect individuals from the fear of violence).
>
> Because we agree with the district court that the messages Fleury sent amount to true threats, they are not afforded protection under the First Amendment. Accordingly, § 2261A(2)(B) is constitutional as applied to Fleury's conduct.

After the Court of Appeals found the indictment sufficient, it held that there was sufficient evidence of the defendant's subjective intent to threaten:

> Viewing the evidence in the light most favorable to the prosecution, there was sufficient evidence of Fleury's subjective intent to threaten. The jury heard from both a defense expert witness, Dr. Butts, and a government expert witness, Dr. Dietz, and they gave conflicting accounts of Fleury's culpability and the effect his ASD had on his ability to comprehend emotions. Specifically, Dr. Dietz concluded that Fleury intended to cause his victims anger, grief, and fear. And, in response to a questionnaire Fleury completed during Dr. Butts's evaluation, Fleury described himself as 'a sympathetic person' and maintained that he 'can put [himself] in other people's shoes.'
>
> After hearing the testimony, the jury was free to determine both experts' credibility as it saw fit. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986) (explaining that '[c]redibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions'). We decline to invade the province of the jury by reevaluating the experts' credibility and reweighing the evidence on appeal. In fact, it is precisely because 'we recognize that 'the jury is free to choose between or among the reasonable conclusions to be drawn from the evidence presented at trial,' [that] our sufficiency review requires only that a guilty verdict be reasonable, not inevitable, based on the evidence presented at trial.' *Browne*, 505 F.3d at 1253.

Moreover, the Eleventh Circuit held that the court below had not committed plain error in allowing the expert testimony of a Government witness, who explained that "Fleury's attraction to the domineering and taunting characteristics of serial killers motivated him to send the intimidating messages and opined that Fleury could appreciate the impact that his messages had on the recipients. This testimony was thus clearly relevant under Rule 401, and Fleury does not explain how the Government failed to meet its burden under Rule 702. While it is true that Dr. Dietz is not an expert on ASD, he is an expert on forensic psychiatry—not solely an expert on mass murderers as Fleury argues on appeal."

Finally, the Court of Appeals found no error in the jury instructions:

> Fleury asserts on appeal that the cyberstalking—or 'interstate stalking'—jury instruction presents an *Elonis* [*v. United States*, 575 U.S. 723 (2015)] issue. He contends that, after *Elonis*, we should hold that a defendant can be constitutionally convicted of making a true threat only if the defendant intended the recipient to feel threatened. The given jury instruction, Fleury argues, does exactly what the Supreme Court held was impermissible in Elonis—defines 'true threat,' and hinges criminal liability, on how a 'reasonable person' would view the messages rather than on the subjective intent of the sender of those messages: the defendant.
>
> We find no error in the instruction provided to the jury. The district court properly declined to instruct the jury that the government had to prove Fleury's subjective intent to communicate a true threat to convict him of cyberstalking under 18 U.S.C. § 2261A(2)(B). Fleury relies in vain on *Elonis*, where the Supreme Court read a mens rea requirement into a statute that lacked *any* scienter element—the transmission of interstate threats under 18 U.S.C. § 875(c). No similar problem exists here because the cyberstalking statute required proof that the defendant acted with the intent to harass or intimidate. *See* 18 U.S.C. § 2261A(2).
>
> Because the plain language of § 2261A(2) establishes a mens rea requirement sufficient 'to separate wrongful conduct from 'otherwise innocent conduct,'' *Elonis*, 575 U.S. at 736, it was not reversible error for the district court to decline to impose an additional, subjective-intent requirement for the jury to convict Fleury of cyberstalking. The jury was instructed on the mens rea element—subjective intent to harass or intimidate—that Fleury must have had while communicating true threats. The jury found the government proved the requisite mental state beyond a reasonable doubt. Fleury cites no case law for his position that, even when a statute contains an express mental state requirement, the district court should read an additional mens rea requirement into the text, nor does such a position make sense. *See United States v. Bell*, 303 F.3d 1187, 1191 (9th Cir. 2002) (declining to include a specific intent instruction when the instruction already included 'the intent to harass,' and concluding that '[t]he instructions given were properly tailored to the charged offense and the district court was not obligated to do more'). Accordingly, we affirm the district court as to this issue. [footnotes omitted].

#Admissibility

#Miscellaneous

United States v. Holmes, Case No. 5:18-cr-00258-EJD-1, 2021 WL 3395146 (N.D. Ca. Aug. 3, 2021)

The defendant was the founder and CEO of Theranos, Inc., which offered blood testing technology. Theranos used a database that housed, among other things, patient test results and quality control data. After the SEC and USDOJ began to investigate Theranos, grand jury subpoenas were issued for a copy of the database, along with the necessary software and access and search it. However, the database was encrypted and a password and private key was needed for access and search. The database was produced by retained counsel without any additional information that would allow access and, having done so, Theranos decommissioned it. In other words, "[t]he parties agree, for all intents and purposes, the LIS database copy produced to the Government cannot be accessed without the private key, and the information on the database is lost—perhaps irretrievably." The defendant moved, among other things, to suppress, arguing that the Government failed to preserve potentially exculpatory evidence. The district court denied the motion to suppress for, among other reasons:

(1) There was no evidence that the defendant ever advised the Government of the purported exculpatory value "either prior to filing the present motion or prior to the decommissioning of the original LIS database."

(2) The information in the database "would not provide a conclusive determination of whether the Theranos blood tests were accurate, and it could just as likely contain incriminating evidence to the contrary. Any exculpatory value is therefore speculative at best."

(3) "The Government thus never had true possession of the LIS database in the first instance, and there is no dispute that the Government played no role in the decommissioning and dismantling of the original LIS database."

(4) "[T]he Government has not failed to preserve evidence so much as it has preserved the unusable evidence Theranos produced. The Government still has the nonfunctioning copy of the LIS, and it has provided Holmes with a copy as well."

The district court also denied the defendant's request for an evidentiary hearing.

#Admissibility

#Discovery Materials

#Encryption

#Preservation and Spoliation

#Trial-Related

United States v. Hunt, 21-CR-86 (PKC), 2021 WL 1428579 (E.D.N.Y. Apr. 15, 2021)

The defendant was indicted for threatening to assault and murder members of Congress. The threats allegedly were made in statements on social media websites. The defendant filed various pre-trial motions. The court ruled, among other things, as follows:

(1) The Government's request to introduce the defendant's *private* text messages was granted "to the extent those messages relate to Defendant's intent when he made the alleged threats." The messages were relevant to the subjective intent requirement under the charging statute. Moreover, "[d]efendant fails to explain why his private statements relating to intent are less relevant than his public statements. Nor are his private messages needlessly cumulative of his public statements; because the private statements may reflect Defendant's views unfiltered for publication, they provide a different perspective of his state of mind than those he made publically."

(2) The Government was permitted to allow expert testimony on the defendant's white supremacist and anti-Semitic views well as on alleged coded references in the Defendant's text messages as these were relevant to the elements of the charging statute. However, "[g]iven the likelihood of undue prejudice, the Government may introduce such evidence only to the extent necessary to explain the meaning of the references in Defendant's alleged threats and Defendant's knowledge of those meanings."

(3) The Government sought leave to introduce certified records of the contents of certain of the defendant's social media accounts. The court held that, "to the extent the Government seeks to authenticate and admit the *content* *** via certifications, such items are not self-authenticating business records that require no extrinsic evidence of authenticity other than a certification from a custodian to be admitted." The court explained: "Where, as here, social media content is offered for the purpose of establishing that a person made particular statements—that is, the relevance of the proffered evidence 'hinges on the fact of authorship'—a certification by a custodian in itself cannot be sufficient for purposes of authentication because *** such a certification serves a limited role: it simply shows that a record was made at

or near a certain time, that the record was kept in the course of a regularly conducted business activity, and that the making of the record was a regular practice of that activity."

(4) In its ruling, the court distinguished the purpose of admission: "Moreover, to the extent that the Government simply seeks to admit records about Defendant's social media content—such as metadata showing times and dates of posting or transmission, or IP addresses, those sorts of records would be self-authenticating." The court rejected the defendant's argument that authenticating records through a certification, rather than through a live witness, violated the Confrontation Clause.

#Admissibility

#Trial-Related

United States v. Johnson, No. 19-4331, 2021 WL 1703605 (4th Cir. Apr. 30, 2021)

The defendants were convicted of distributing heroin that, when used, led to the death of an 18-year-old and were also convicted of distributing heroin to an individual. On appeal, they argued, among other things, that the Government failed to disclose and preserve the 18-year-old's cell phone. Evidence against the defendants included "activities surrounding the sale [that] were documented in a video shared on the social media service Snapchat – but the defendants have disputed that the substance was heroin" and caused the death. The Government had possession of the phone but returned it to the decedent's family after one defendant pled guilty before a magistrate judge and before a district judge rejected the plea agreement. That defendant sought the cell phone after rejection of the agreement to defend against a "death count" through service of a subpoena on the decedent's family. However, the family "misplaced the phone after receiving it from the Government and thus could not produce it." The district court denied a defense request to dismiss the death count and for a spoliation instruction. The Court of Appeals reversed and remanded for an evidentiary hearing given all the circumstances:

> As we see it, however, the evidentiary record is too meager to render a proper ruling on Johnson and Stewart's due process claim. And the deficiency of the record is not limited to the *Youngblood* bad faith issue; it also inhibits the application of *Brady, Agurs, Trombetta,* and the potentially-useful-evidence standard of *Youngblood*. Consequently, we must conclude that the district court erred by rejecting the defendants'

claim in reliance on an incomplete record – a record that was even more inadequate at the time of the district court's ruling than it is now that it includes the trial evidence.

Simply put, much remains unknown regarding the circumstances of the Government's failure to disclose and preserve Medrano's [the decedent's] cell phone. For example, even if Investigator Bean did not review the contents of the cell phone, did Deputy Whitehead or another police officer or a prosecutor or witness do so? What did Medrano's family see on the cell phone when they looked through its photographs? What is Bean's sworn explanation for returning the cell phone to Medrano's family? Did Bean actually believe the case was over because Johnson had entered a guilty plea to the Distribution Count? Did Bean consider that Johnson's plea agreement had not been accepted by the district court and that the Death Count remained pending? Did Bean consider Stewart and the pendency of the Death Count as to her? Did it concern Bean that there had not been any convictions, sentencings, or appeals in the case? Did Bean consult the prosecutors or other police officers before returning the cell phone to Medrano's family? Did Bean dispose of additional Death Count evidence or only the cell phone?

These are important questions that need to be answered in order for a fair and appropriate analysis of Johnson and Stewart's due process claim to be conducted. Thus, we cannot ratify the district court's approach of disallowing witnesses and then relying on the limited evidentiary record to reject the defendants' claim.

Indeed, we also have doubts about the merits of the district court's decision. Specifically, we are troubled by the court's narrow focus on *Youngblood* and the court's ruling that Investigator Bean acted neither in bad faith nor even negligently in returning Medrano's cell phone because he 'held on to it until after [Johnson's] change of plea hearing.' *** It confounds us how the court could accept it as reasonable for Bean to believe the case was over upon Johnson's guilty plea to the Distribution Count, but unreasonable for Johnson not to request the cell phone as evidence on the Death Count prior to the court's rejection of his plea agreement. We are also troubled by the court's pronouncement that there was only 'potentially useful evidence on that phone,' *** as the Government conceded that the cell phone had at least some content with apparent exculpatory value, i.e., the "laced blunt" text indicating that Medrano smoked a laced blunt in addition to snorting the defendants' alleged heroin shortly before his death.

In any event, the district court will have the opportunity to reassess Johnson and Stewart's due process claim with the expansion of the

> evidentiary record on remand. We fully expect that the additional evidence — including evidence elucidating Investigator Bean's decision to return Medrano's cell phone and delineating the cell phone's known and suspected contents — will enable a thorough analysis of the due process claim that includes a careful application of the principles of *Brady*, *Agurs*, *Trombetta*, and *Youngblood*. Such an analysis is plainly merited, as the defendants have stated a plausible claim that the Government's failure to disclose and preserve the cell phone has impeded their ability to defend themselves on the Death Count by showing that drugs other than the defendants' alleged heroin may have caused Medrano's death. Although the defendants would be entitled to due process with respect to any criminal charge, it bears repeating that the Death Count carries a mandatory sentence of 20 years to life. [footnote omitted].

The Fourth Circuit also made some "observations" on an adverse inference instruction should there be a retrial, including this:

> Upon any retrial on remand, the district court should entertain ways to inform the jury of the Government's loss of Medrano's cell phone without revealing Johnson's guilty plea so that an adverse inference instruction may be given. The court should also consider that the existing record reflects the following: that Investigator Bean has admitted knowing early in the investigation that the cell phone contained evidence relevant to the issue of whether Medrano's death resulted from the use of Johnson and Stewart's alleged heroin or other drugs from other sources; that despite his knowledge of the cell phone's evidentiary value, Bean intentionally returned the cell phone to Medrano's family after opting not to analyze it; and that the family then misplaced the cell phone, preventing the defendants from presenting the cell phone's lost contents to establish a reasonable doubt that their alleged heroin was a but-for cause of Medrano's death. Finally, to the extent that the court may be inclined to again charge the jury as it did during the June 2018 trial, the court should consider whether an instruction on weaker or less satisfactory evidence — being based on the Government's failure to analyze the cell phone, with no explanation to the jury that the cell phone is now lost and cannot be analyzed by the defendants or anyone else — is truly an adequate substitute for an adverse inference instruction.

#Admissibility

#Discovery Materials

#Preservation and Spoliation

#Trial-Related

United States v. Korf, No. 20-14223, 2021 WL 3852229 (11th Cir. Aug. 30, 2021) (*per curiam*)

This matter arose out of a criminal investigation into money laundering in the Northern District of Ohio. The Government secured a warrant to search a suite of offices in the Southern District of Florida in aid of the investigation. Seized documents contained items that were alleged to be protected by the attorney-client privilege. The warrant included a protocol concerning the handling of such materials. Various individuals and business entities moved to intervene and for injunctive relief related to the use of a taint team in the protocol. The issuing magistrate judge conducted a hearing on the request for injunctive relief and modified the protocol. The district judge affirmed and the intervenors sought appellate relief. The Eleventh Circuit held that the order in issue (the district court's affirmance) was final and appealable and that injunctive relief was not warranted:

> Though the magistrate judge originally approved the Original Filter-Team Protocol *ex parte*, before the investigative team could review any documents, the court held an adversarial hearing and, after considering the Intervenors' concerns, put the Modified Filter-Team Protocol into place. Also ***, this case involves no claims that the majority of seized materials were both privileged and irrelevant to the subject of the investigation. And finally, the Modified Filter-Team Protocol did not assign judicial functions to the executive branch. Rather, and as we have noted, under the Modified Filter-Team Protocol, the Intervenors have the first opportunity to identify potentially privileged materials. And before any of those items may be provided to the investigative team, either the Intervenors or the court must approve. Put simply, the Modified Filter-Team Protocol complies with the recommendations both the Sixth and Fourth Circuits have made concerning the use of filter teams.
>
> So once again, we return to the observation that the Modified Filter-Team Protocol appears to us to comply with even the most exacting requirements other courts that have considered such protocols have deemed appropriate. In short, the Intervenors have not clearly established a substantial likelihood of success on the merits. [footnote omitted].

#Discovery Materials

#Miscellaneous

United States v. Lamm, No. 20-1128, 2021 WL 3196472 (8th Cir. July 29, 2021)

The defendant was convicted of child pornography-related offenses. On appeal, he challenged, among other things, the admission of certified records from Facebook that showed he operated two Facebook accounts. The Government sought to have the records self-authenticated under Rule 902(11). The district court required the Government to offer extrinsic evidence under Rule 901(a). The defendant argued on appeal that the records had not been authenticated and contained hearsay. The Court of Appeals affirmed. First, with regard to authentication:

> '[A]uthentication of social media evidence . . . presents some special challenges because of the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter.' *United States v. Browne*, 834 F.3d 403, 412 (3d Cir. 2016). Our circuit has not yet considered what is sufficient authentication for evidence from social media accounts. Several other circuits have dealt squarely with the issue and have held that certification from the social media forum is insufficient to establish authenticity under Federal Rule of Evidence 902(11), and more extrinsic evidence is required to establish authenticity under Rule 901(a). *See, e.g.*, *Browne*, 834 F.3d at 405.
>
> ***
>
> We agree with the Third and Seventh Circuits: the Government may authenticate social media evidence with circumstantial evidence linking the defendant to the social media account. The Government did that here. First, the Government linked the same cell phone number—in Kevin Lamm's name—to both accounts. Second, the same *images that appeared on Lamm's Facebook account appeared on the Malone account. See [United States v.] Lewisbey*, 843 F.3d at 658. Third, Lamm had copies of those images on memory cards in his apartment. Fourth, those same memory cards also contained screenshots of private messages only the Malone account could access. Fifth, other online subscriptions found on Lamm's computer used an email address containing the name Mike Malone. Taken together, this evidence provided a rational basis for the district court to pass the question of authentication to the jury. [footnotes omitted].

The Eighth Circuit then rejected the defendant's hearsay argument, ruling that the statements were not offered by the Government for their truth but were instead offered to provide "context" for his responses contained in the exhibits.

#Admissibility

#Trial-Related

United States v. Meals, No. 20-40752, 2021 WL 6143550 (5th Cir. Dec. 30, 2021)

The defendant used a Facebook messaging app to discuss sexual encounters with a minor. Facebook discovered the conversations and forwarded these to the NCMEC which, in turn, reported the conversations to law enforcement, which secured a warrant for the defendant's electronic devices. Child pornography was found. After the defendant was charged, he moved unsuccessfully to suppress, arguing that Facebook and NCMEC were government agents and had conducted a warrantless search. The defendant then pled guilly and repeated his argument on appeal. The Fifth Circuit affirmed under the "private search doctrine:" (1) Although federal law requires platforms such as Facebook to report child expoitation to NCMEC, "it neither compels nor coercively encourages internet companies to search actively for such evidence." (2) Given this, the defendant's argument "falls flat." (3) Assuming that NCMEC was a government agent, it "did not exceed the scope of Facebook's search by merely reviewing the identical evidence that Facebook reviewed and placed in a cyber tip." The Fifth Circuit also rejected the defendant's argument that the district court had erred in applying the "reasonable expectation of privacy" test rather than the "chattel trespass" test of *United States v. Jones*, 565 U.S. 400 (2012), when it evaluated his claim that NCMEC had violated his Fourth Amendment rights.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

United States v. Moore-Bush, 982 F.3d 50 (1st Cir. 2020), granting pet. for en banc rehearing and vacating judgment of panel below.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

United States v. Moses, 6:19-CR-06074 EAW, 2021 WL 4739789 (W.D.N.Y. Oct. 12, 2021)

The defendant was charged with multiple counts of mail and wire fraud as well as other offenses. The trial court expressed an intent to excuse from the pool of prospective jurors any persons not vaccinated against COVID-19. The defendant did not object. However, the Government did, because doing so would "violate the

fair cross-section requirement of the Constitution and the Jury Selection and Service Act." The court disagreed, concluding that the unvaccinated were not a "distinctive group" for fair cross-section purposes, the unvaccinated could not be considered a "proxy for a distinctive group," and the presence of unvaccinated jurors would present a substantial risk likely to disrupt the trial "given the anticipated legnth of this trial and the high levels of community transmission currenty present in the relevant counties [from which prospective jurors would be called], combined with the fact that the size and configuration of the courtroom *** do not allow for social distancing ***."

#Miscellanous

#Trial-Related

United States v. Ramirez-Mendoza, No. 4:20-CR-00107, 2021 WL 4502266 (M.D. Pa. Oct 1, 2021)

The defendant was charged with possession with intent to distribute and with illegal reentry. She moved to suppress evidence obtained as a result of the search of her vehicle and statements made during a traffic stop. After the defendant's vehicle was stopped for suspected illegal window tinting, the arresting officer observed two cell phones and a single key in the ignition. He also detected the "strong odor of air freshener." The officer used Google Translate to speak with the defendant, whose primary language was Spanish. He became suspicious of the defendant for several reasons. The district court found that the officer and the defendant were able to communicate with Google Translate "reasonably well despite some confusion arising from apparent mistranslations." The officer searched the vehicle, found fentanyl, and arrested the defendant. The court found that the Government had not met its burden to prove that the defendant had consented to the warrantless search. Among other things, the court was not convinced that Google Translate accurately translated the officer's request into Spanish and declined to "infer that Google Translate accurately translated and communicated Conrad's [the officer's] request to search Ramirez-Mendoza's vehicle solely because it may work well *generally*." However, the court did find that the warrantless search fell within the "automobile exception" to the Warrant Requirement because the circumstances surrounding the stop were sufficient to establish probable cause.

#Fourth Amendment – Good Faith exception

#Fouth Amendment – Warrant Required or Not

#Miscellaneous

United States v. Oliver, 987 F.3d 794 (8th Cir. 2021)

The defendant was convicted on five counts of drug trafficking. He argued on appeal, among other things, that the district court had erred in admitting certain maps into evidence. The Court of Appeals affirmed the convictions but reversed and remanded for resentencing. In affirming, it rejected the defendant's argument about the maps:

> Oliver challenges the admission into evidence of a series of maps offered to establish that the controlled buys took place within 1,000 feet of a 'protected location.' *** Two Sioux City employees—Geographic Information Systems Supervisor Nicholas Bos and Crime Analyst Marie Divis—created the maps to depict the location of each drug transaction relative to nearby parks or schools. Based on statements made by Sergeant Troy Hansen from the Sioux City Police Department, Bos and Divis used mapping software to electronically mark the relevant locations on maps and then noted the distances between them with lines and other labels.
>
> Oliver argues the map exhibits are inadmissible because Bos and Divis's markings (or 'tacks') on the maps constitute hearsay. Hearsay is 'a statement that . . . the declarant does not make while testifying at the current trial or hearing; and . . . [that] a party offers in evidence to prove the truth of the matter asserted in the statement.' Fed. R. Evid. 801(c). Hearsay is generally inadmissible 'unless one of several exceptions applies.' United States v. Hemsher, 893 F.3d 525, 533 (8th Cir. 2018) (citing Fed. R. Evid. 802). According to Oliver, the markings designating the locations of the parks, schools, and drug transactions 'reflect out-of-court statements' made by Sergeant Hansen to Bos and Divis. The government disagrees but does not rely on any hearsay exception. Instead, the government argues that the markings are not hearsay at all because (1) Bos, Divis, and Sergeant Hansen all testified at trial and were subject to cross-examination, and (2) the markings on the maps were generated by computer software, not placed manually.
>
> The fact that Bos, Divis, and Hansen testified at trial does not tell us whether the maps contained hearsay. Rather, the question is whether the markings on the maps are statements that 'the declarant d[id] not make while testifying at trial.' See Fed. R. Evid. 801(c). Indeed, it is undisputed that, before trial, Sergeant Hansen provided the addresses of

> the controlled drug transactions and the relevant protected locations to Bos and Divis, who then used that information to create the map exhibits. The government also agrees that it used the maps to show that the controlled buys occurred within 1,000 feet or less of a protected location, an element of all five counts that had to be proven beyond a reasonable doubt. Sergeant Hansen's statements regarding where to place the marks were made out-of-court. And they were then offered by the government at trial for the truth of the matter asserted: the locations of the parks, schools, and drug transactions. ***
>
> We are not persuaded by the argument that the markings cannot constitute hearsay simply because they are computer-generated. Although '[m]achine-generated records usually do not qualify as 'statements' for hearsay purposes,' they 'can become hearsay when developed with human input.' United States v. Juhic, 954 F.3d 1084, 1089 (8th Cir. 2020) (citing Melendez-Diaz v. Massachusetts, 557 U.S. 305, 310-11 (2009)). In Juhic, this court determined that computer-generated reports contained impermissible hearsay because 'human statements and determinations were used to classify' the relevant files that were referenced in the reports and later offered against the defendant. Id. at 1088-89. Similarly, here, Sergeant Hansen's out-of-court statements regarding the physical locations of the drug transactions were used to produce the relevant points and distances marked on the maps. Bos also testified that he added a legend to each map describing the relevant locations. See id. at 1089 ('The human involvement in this otherwise automated process makes the notations hearsay.').
>
> But even assuming it was error to admit the maps because they contained hearsay, any error was harmless. *** Here, the maps were not the only evidence that showed the proximity of the drug transactions to a protected location. Rather, the maps were duplicative of properly admitted photographs and in-court testimony from Hansen, Bos, and Divis. In short, the jury did not need to rely on the maps to find that Oliver engaged in drug transactions within 1,000 feet of a protected location. *** [footnotes omitted].

In its ruling, the Eighth Circuit commented on *United States v. Lizarraga-Tirado*, 789 F.3d 1107 (9th Cir. 2015):

> The government urges us to follow the reasoning in United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109-10 (9th Cir. 2015), in which the Ninth Circuit held that a Google Earth satellite image containing 'tacks' marking certain GPS coordinates was not hearsay because although a human had to type in the coordinates, the 'tacks' were automatically generated by the software. Lizarraga-Tirado is not only inconsistent with

> Juhic, it is also factually distinguishable from Oliver's case. The maps at issue here contain more than computer-generated tacks—they also have human-created labels, titles, and lines indicating distance.

#Admissibility

United States v. Tuggle, No. 20-2352, 2021 WL 2946100 (7th Cir. July 14, 2021)

The defendant was under investigation for participation in a methamphetamine distribution conspiracy. As part of the investigation, three video cameras were attached to utility poles to monitor his residence for an 18-month period. Relying on evidence obtained from the cameras, the Government secured warrants to search the residence. The defendant was indicted on drug-related offenses and moved to suppress the evidence derived from the cameras, arguing that their use was a warrantless search. The district court denied the motion and the defendant entered a conditional guilty plea. On appeal, the Seventh Circuit affirmed:

> Tuggle's case presents an issue of first impression for this Court: whether the warrantless use of pole cameras to observe a home on either a short- or long-term basis amounts to a "search" under the Fourth Amendment. The answer—and even how to reach it—is the subject of disagreement among our sister circuits and counterparts in state courts. Their divergent answers reflect the complexity and uncertainty of the prolonged use of this technology and others like it. Nevertheless, most federal courts of appeals that have weighed in on the issue have concluded that pole camera surveillance does not constitute a Fourth Amendment search.
>
> Ultimately, bound by Supreme Court precedent and without other statutory or jurisprudential means to cabin the government's surveillance techniques presented here, we hold that the extensive pole camera surveillance in this case did not constitute a search under the current understanding of the Fourth Amendment. In short, the government's use of a technology in public use, while occupying a place it was lawfully entitled to be, to observe plainly visible happenings, did not run afoul of the Fourth Amendment. Therefore, we affirm the district court's denial of Tuggle's motion to suppress.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

United States v. Wilson, No. 18-50440, 2021 WL 4270847 (9th Cir. Sept. 21, 2021)

Here is the summary of this lengthy opinion:

> The panel vacated a conviction for possession and distribution of child pornography, reversed the district court's denial of a motion to suppress, and remanded for further proceedings in a case in which the panel addressed whether the government's warrantless search of the defendant's email attachments was justified by the private search exception to the Fourth Amendment.
>
> As required by federal law, Google reported to the National Center for Missing and Exploited Children (NCMEC) that the defendant had uploaded four images of apparent child pornography to his email account as email attachments. No one at Google had opened or viewed the defendant's email attachments; its report was based on an automated assessment that the images the defendant uploaded were the same as images other Google employees had earlier viewed and classified as child pornography. Someone at NCMEC then, also without opening or viewing them, sent the defendant's email attachments to the San Diego Internet Crimes Against Children Task Force, where an officer ultimately viewed the email attachments without a warrant. The officer then applied for warrants to search both the defendant's email account and his home, describing the attachments in detail in the application.
>
> The private search doctrine concerns circumstances in which a private party's intrusions would have constituted a search had the government conducted it and the material discovered by the private party then comes into the government's possession. Invoking the precept that when private parties provide evidence to the government on their own accord, it is not incumbent on the police to avert their eyes, the Supreme Court formalized the private search doctrine in *Walter v. United States*, 447 U.S. 649 (1980), which produced no majority decision, and *United States v. Jacobson*, 466 U.S. 109 (1984), which did.
>
> The panel held that the government did not meet its burden to prove that the officer's warrantless search was justified by the private search exception to the Fourth Amendment's warrant requirement. The panel wrote that both as to the information the government obtained and the additional privacy interests implicated, the government's actions here exceed the limits of the private search exception as delineated in *Walter* and *Jacobsen* and their progeny. First, the government search exceeded the scope of the antecedent private search because it allowed the government to learn new, critical information that it used first to obtain a

> warrant and then to prosecute the defendant. Second, the government search also expanded the scope of the antecedent private search because the government agent viewed the defendant's email attachments even though no Google employee—or other person—had done so, thereby exceeding any earlier privacy intrusion. Moreover, on the limited evidentiary record, the government has not established that what a Google employee previously viewed were exact duplicates of the defendant's images. And, even if they were duplicates, such viewing of others' digital communications would not have violated the defendant's expectation of privacy in his images, as Fourth Amendment rights are personal. The panel concluded that the officer therefore violated the defendant's Fourth Amendment right to be free from unreasonable searches when he examined the defendant's email attachments without a warrant.

The Court of Appeals also addressed *Carpenter* in a footnote:

> Wilson opines that the private search exception to the Fourth Amendment should be overruled, and seeks to preserve that question for any Supreme Court review of this case. As a court of appeals, we of course cannot overrule Supreme Court cases. *** We do note that the private search doctrine rests directly on the same precepts concerning the equivalence of private intrusions by private parties and the government that underlie the so-called third-party doctrine. *** In *Jacobsen*, the Supreme Court reasoned that the private search exception follows from the premise, underlying the third-party doctrine, that 'when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities.' 466 U.S. at 117. In recent years, however, the Court has refused to 'mechanically apply[] the third-party doctrine,' stressing that 'the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'' *Carpenter*, 138 S. Ct. at 2219 (quoting *Riley*, 573 U.S. at 392); *see United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (explaining that the third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"); Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 Harv. L. Rev. 205, 224 (2018) (noting that *Carpenter* 'significantly narrowed the [third-party] doctrine's scope').

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Third-Party Doctrine

Villarreal v. City of Laredo, No. 20-40359, 2021 WL 5049281 (5th Cir. Nov. 1, 2021)

This was a Section 1983 action brought by a journalist who posted her work on Facebook. After she posted about a man who committed suicide in which she revealed his name and that he was a Border Patrol agent and posted the last name of a family involved in a fatal car accident, arrest warrants were issued for the plaintiff for violations of a Texas Penal Code provision that made it a crime to solicit or receive information from a public official that the official had access to and had not been made public. The plaintiff had contacted a police officer who, on both occasions, had verified information the plaintiff had obtained elsewhere. The plaintiff turned herself in and during booking, images were taken of her in handcuffs on cell phones and she was mocked and laughed at by police officers. She was then detained. A state judge granted her *habeas* relief on the grounds that the charging statute was unconstitutionally vague. Thereafter, she filed the 1983 action against the officers for infringing her rights to ask questions of public officials and for arresting her in retaliation for doing so. The district judge dismissed the 1983 action, concluding, among other things, that the individual defendants were entitled to qualified immunity. The Court of Appeals reversed as to the individual defendants. The appellate panel held, among other things, that, "it should have been patently obvious to any reasonable police officer that the conduct alleged in the complaint constitutes a blatant violation of Villarreal's constitutional rights" under the First and Fourth amendments and, accordingly, qualified immunity was unavailable.

#Fourth Amendment – Good Faith Exception

#Miscellaneous

DECISIONS – STATE

City of Seattle v. Buford-Johnson, No. 81627-6-1, 2021 WL 6112342 (Wash. Ct. App. Div. 1 Dec. 27, 2021)

The defendant was arrested after he drove past a Seattle police officer and yelled "f*** the police" while pointing as if he had a weapon. He was found guilty of harassment under Washington State law. On appeal, the defendant argued that the

evidence had not established that he had made a true threat. The Court of Appeals agreed:

> Here, we conclude that the evidence does not establish that Johnson made a true threat. Whether Johnson's speech was a true threat directly determines whether his speech was unprotected, so we engage in an independent review of the crucial facts. We start by looking to the words Johnson spoke: Johnson's statement did not itself express any intention to cause harm, but instead was a generalized and political statement of animosity. We have noted that 'criticism, commentary, and even political hyperbole towards and about public servants' is political speech that is at the core of First Amendment protection 'no matter how vehement, caustic[,] and sometimes unpleasantly sharp.' *** The trial court therefore appropriately concluded that Johnson's language itself was protected speech. However, Johnson also pointed at Officer Zerr as if he had a firearm, expressive conduct that does imply violence. The City correctly notes that mimicking the firing of a gun has been considered threatening in other contexts and jurisdictions. See, e.g., Haney v. U.S., 41 A.3d 1227, 1234 (2012) (defendant miming shooting a gun at a witness and mouthing "I'm going to fuck you up" could reasonably be considered a threat). We must therefore examine 'all the facts and circumstances' to determine whether Johnson's conduct constituted a threat in this case. [State v.] C.G., 150 Wn.2d at 611.
>
> The circumstances here do not convince us that Johnson's speech and conduct together constituted a true threat. Johnson did not stop or approach Officer Zerr, but instead continued driving north throughout the interaction. Furthermore, Johnson kept his arm hanging out of the window of the car as he continued to drive, and then immediately stopped at a red light. These facts are more suggestive of a casual encounter or idle talk than a serious threat. [footnotes omitted].

#Miscellaneous

Commonwealth v. Carrasquillo, SJC-13122 (Mass. Feb. 7, 2022)

At issue here was "the novel question whether the defendant had a constitutionally protected expectation of privacy in social media content that he shared, albeit unknowingly, with an undercover police officer." The defendant accepted a "friend" request from the officer on Snapchat. Thereafter, the defendant posted a video of a person holding what may have been a weapon. The officer recorded the posting, which was used against the defendant in a prosecution for multiple weapons offenses. The defendant moved to suppress the recording, arguing that it

was the result of an unconstitutional search. A motion judge found that the defendant had not shown a subjective expectation of privacy and that, even if he had, the expectation would not have been reasonable. The defendant then entered a conditional plea and appealed the denial of his motion. The Massachusetts Supreme Judicial Court affirmed. The court declined to adopt any bright-line rule regarding the posting of content onto a social media platform. Instead, the court concluded that, under the circumstances before it, the defendant did not have a reasonable expectation of privacy such that "no search in the constitutional sense occurred."

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Social Media

#Third-Party Doctrine

Commonwealth v. Davis, 487 Mass. 448, 168 N.E.3d 294 (2021)

The defendant was convicted of armed assault with intent to murder and related offenses. He was on probation for a federal drug charge and wearing a GPS ankle monitor at the time of the assault. Data from that device "showed he was at the location where the shooting took place very close in time to the shooting, and his speed matched the shooter's movements, according to surveillance video" and the testimony of a witness. On appeal, he challenged, among other things, the admissibility of the GPS evidence. The Supreme Judicial Court held that the GPS evidence as to speed was not sufficiently reliable to be admitted, vacated the defendant's convictions, and remanded for further proceedings given the prejudicial effect of the admission of the speed evidence:

> The defendant's objection at trial and his argument on appeal pertain to the reliability of the ET1 device specifically. He argues that the ET1 does not meet the requirements of Daubert-Lanigan. Chief among the defendant's concerns is the fact that the ET1's ability to measure speed has never been formally tested. Given the complete lack of formal testing of the ET1 model for speed, there is also no known error rate. Moreover, the defendant asserts that because the ET1 is proprietary, it is impossible to say whether the methodology it employs is generally accepted. The proprietary nature also means it has not been subject to peer review. Finally, its accuracy is not governed by any recognized standards.

> We agree with the defendant that if a new model of a device is objected to on reliability grounds, it must pass gatekeeper reliability under either Daubert-Lanigan or Frye. It is not sufficient to show merely that GPS technology is, in general, reliable without making any showing pertaining to the reliability of a particular model of a device. The Commonwealth could meet that burden by showing that the new model itself satisfies the Daubert-Lanigan factors -- for example, that it has been tested or peer reviewed. That is not the only way, however, to show that a new model is reliable. For example, if an older model has previously been found reliable, the proponent need only show that the new model applies the same methodology as that prior one. Given that devices generally tend to improve, that will generally be sufficient to show that the new device, too, is reliable. Here, the Commonwealth made neither showing. It only showed that the GPS technology is a reliable theory. For the speed data, it has not shown that the ET1 itself -- either through testing or through its similarity to a generally accepted device -- reliably applies that accepted theory. Thus, the judge abused his discretion in admitting the ET1 speed evidence.
>
> Because on retrial the Commonwealth may again attempt to lay the proper foundation for the speed evidence, we comment on the remainder of the analysis. If the Commonwealth attempts to show that a new model of a device is reliable by asserting that it is similar to a prior model, the defendant may object and move for a Daubert-Lanigan hearing on the new device. This is essentially what occurred in Camblin I, 471 Mass. at 642. There, the Commonwealth sought to introduce evidence from a particular model of breathalyzer (Alcotest) that had not previously been reviewed by our courts. *** The defendant moved for discovery of the device's computer source code, and that request was granted pursuant to a nondisclosure agreement. *** The defendant retained experts to examine the source code. *** The defendant then filed affidavits and reports contending that the source code contained thousands of errors and argued that the Alcotest used methods different from previous machines that had been reviewed by our courts. *** On appeal, we held that because neither statute nor existing case law offered guidance about the reliability of the Alcotest's methodology, the judge should have held a Daubert- Lanigan hearing. *** We remanded the case for that hearing, and then, in Camblin II, 478 Mass. at 469-470, held that the judge did not abuse his discretion in finding that the Alcotest satisfied the Daubert-Lanigan standard. [footnotes omitted].

The court also commented on the role of the trial judge:

> Given that the issue could also arise on retrial, we briefly comment on the difference between gatekeeper reliability and conditional relevance in this scenario. If the defendant objects -- as he did here -- to the reliability of the ET1 model as a whole, then the Commonwealth bears the burden of showing that the ET1 passes gatekeeper reliability. See Mass. G. Evid. §§ 104(a), 702. See, e.g., Camblin I, 471 Mass. at 640 (reliability of Alcotest device). On the other hand, if the defendant objects to whether the specific ET1 device worn by the defendant on September 15, 2015, was functioning properly, then the issue is likely a matter of conditional relevance, for which the Commonwealth also bears the burden of laying the proper foundation. See Mass G. Evid. § 104(b). See, e.g., Commonwealth v. Torres, 453 Mass. 722, 737 (whether measuring device was calibrated); Commonwealth v. Neal, 392 Mass. 1, 19 (1984) (whether particular breathalyzer unit was accurate at time test was performed); Commonwealth v. Whynaught, 377 Mass. 14, 17 (1979) (whether individual radar speedmeter was calibrated); Commonwealth v. Podgurski, 81 Mass. App. Ct. 175, 185-186, 961 N.E.2d 113 (2012) (whether individual scale was calibrated).

The Supreme Judicial Court also addressed the defendant's argument that the trial court had erred in admitting maps that depicted the GPS evidence of the defendant's movement as doing so violated his Sixth Amendment and Massachusetts equivalent rights of confrontation and constituted hearsay:

> At trial, the Commonwealth introduced maps showing the defendant's latitude and longitude points reported from the ET1 from 10:25 A.M. to 10:32 A.M. Buck testified that the maps were created by BI collecting the latitudes and longitudes of GPS points over time and sending them to a third-party mapping company. The mapping company would then produce a map encompassing all the points. Finally, BI would plot the points onto the map. Although the record is not entirely clear how the points are plotted on the map, it appears they are generated by a computer.
>
> 'Hearsay requires a 'statement,' i.e., 'an oral or written assertion or ... nonverbal conduct of a person, if it is intended by the party as an assertion.'' Commonwealth v. Thissell, 74 Mass. App. Ct. 773, 776-777 (2009), S.C., Thissell II, 457 Mass. 191, 928 N.E.2d 932, quoting Commonwealth v. Whitlock, 74 Mass. App. Ct. 320, 326 (2009). See Mass. G. Evid. § 801(a). Whether a computer record contains a statement depends on whether the record is 'computer-generated,' 'computer-stored,' or a hybrid of both. Thissell II, supra at 197 n.13. Computer-generated records are created solely by the mechanical operation of a computer and do not require human participation.

> Commonwealth v. Royal, 89 Mass. App. Ct. 168, 171-172 (2016). For this reason, they cannot be hearsay.
>
> With the exception of the defendant's name, all of the information included in the maps was computer-generated. The latitude, longitude, and speed points in the text boxes were generated by the GPS technology. The maps themselves were rendered by a computer at the third-party mapping company. And the dots on the map were rendered by BI's computer system. Thus, because the maps -- with the exception of the defendant's name -- were computer generated, they do not contain a statement and are not hearsay. Further, because the maps were not hearsay, they did not violate the confrontation clause. See Pytou Heang, 458 Mass. at 854, citing Commonwealth v. Hurley, 455 Mass. 53, 65 n.12 (2009). [footnotes omitted].

#Admissibility

#CSLI

#Sixth Amendment – Right of Confrontation

#Trial-Related

Commonwealth v. Delgado-Rivera, 487 Mass. 551, 168 N.E.3d 1083 (2021)

The defendant and others were indicted for drug trafficking. The indictments followed an investigation during which evidence was acquired from the search of a codefendant's cell phone. The defendant attempted to join the owner of the phone in a motion to suppress. A motion judge allowed the defendant to do so. The Supreme Judicial Court reversed, concluding that the defendant had no reasonable expectation of privacy under either the Fourth Amendment or its Massachusetts equivalent in text messages that were sent by the defendant and stored on a phone that belonged to and was possessed by another because he "assumed the risk that the communications he shared *** might be made accessible to others ***." The court did not address how various technologies might change its conclusion:

> The question whether an individual could use certain types of technologies, such as encryption or ephemeral messaging, to maintain control of sent electronic messages sufficiently to retain a reasonable expectation of privacy in those messages is not before us. Cf. WhatsApp Inc. v. NSO Group Techs. Ltd., 472 F. Supp. 3d 649, 659 (N.D. Cal. 2020) ; Nield, The best apps to send self-destructing messages, Popular Science (Nov. 15, 2020), https://www.popsci.com/send-self-destructing-messages.

The court also noted another question:

> An individual's reasonable expectation of privacy in information held by third parties, such as telephone companies, is a separate and distinct question that is not at issue here. See, e.g., Commonwealth v. Fulgiam, 477 Mass. 20, 34, cert. denied, —— U.S. ——, 138 S. Ct. 330 (2017) (recognizing objectively reasonable expectation of privacy in content of defendant's text messages stored by cellular telephone service provider); Commonwealth v. Augustine, 467 Mass. 230, 241-255, S.C., 470 Mass. 837 and 472 Mass. 448 (2015) (recognizing objectively reasonable expectation of privacy in defendant's historical cell site location information records held by telephone service provider).

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Reasonable Expectation of Privacy

#Trial-Related

Commonwealth v. Yusuf, 488 Mass. 379 (2021)

While responding to a call about a domestic disturbance at the defendant's home, a police officer made a digital recording of the encounter with his body-worn camera that captured "intimate details of the parts of the home" through which the officer moved. The footage was stored by the police and later retrieved and reviewed, without a search warrant, in connection with "an independent investigation to confirm a suspicion that the defendant was engaged in criminal activity." Based on that review, the police secured a warrant to search the home and, in doing so, found a weapon and ammunition. The defendant's motion to suppress was denied. The defendant was then convicted of unlawful possession of the firearm and possession of the ammunition without a firearm identification card. The Supreme Judicial Court vacated the order denying the motion to suppress and remanded:

> This case presents two issues of first impression in Massachusetts: first, whether the warrantless use of the body-worn camera that recorded the interior of the home, the most sacred, constitutionally protected area, comprised a violation of the Fourth Amendment to the United States Constitution or art. 14 of the Massachusetts Declaration of Rights; and, second, whether the subsequent review of the footage obtained, for investigative purposes unrelated to the incident giving rise to its creation, constituted a warrantless search.

> We conclude that the use of the body-worn camera within the home was not a search in the constitutional sense, because it documented the officer's plain view observations during his lawful presence in the home. The later, warrantless, investigatory review of the video footage, however, unrelated to the domestic disturbance call, was unconstitutional. That review resulted in an additional invasion of privacy, untethered to the original authorized intrusion into the defendant's home; absent a warrant, it violated the defendant's right to be protected from unreasonable searches guaranteed by the Fourth Amendment and art. 14.
>
> The record is insufficient to determine whether the Commonwealth met its burden to establish that the decision to seek the search warrant was not prompted by the unlawful review of the video footage. See Commonwealth v. Pearson, 486 Mass. 809, 813-814 (2021). Therefore, the order denying the motion to suppress must be vacated and set aside, and the matter remanded to the Superior Court for further proceedings.

#Fourth Amendment – Warrant Required or Not

Ex Parte Jones, No. PD-0552-18, 2021 WL 2126172 (Tex. Ct. Crim. App. May 26, 2021)

> There does not seem to be a dispute that the classic 'revenge porn' scenario—two people take intimate sexual photographs, and one person decides to post them on the Internet without the consent of the other—could be a viable set of facts to support the prosecution of the person who disseminates the pictures. But what about when someone who wasn't involved in that encounter sees the pictures and shares them with other people? Can the State prosecute that person without violating the First Amendment? That is the difficulty with analyzing Section 21.16(b) of the Penal Code, at least as it existed in 2017. But, interpreting Section 21.16(b) as alleged in the indictment, we hold that the statute only covers the intentional disclosure of sexually explicit material by third parties when that third party (1) obtained the material under circumstances in which the depicted person had a reasonable expectation that the image would remain private; (2) knew or was aware of but consciously disregarded a substantial and unjustifiable risk that he did not have effective consent of the depicted person; and (3) knowingly or recklessly identified the depicted person and caused that person harm through the disclosure. Properly construed, the statute does not violate the First Amendment. We reverse the court of appeals. [footnote omitted].

#Miscellaneous

People v. Blanco-Ortiz, 2021 NY Slip Op 04447 (App. Div. 4th Dept. July 16, 2021) (mem.)

The defendant appealed from the imposition of various conditions of probation following his conviction for attempted sexual abuse in the first degree. The appellate court struck two conditions:

> We agree with defendant, however, that the court erred in imposing the remainder of condition 34 and condition 35. In addition to prohibiting defendant from maintaining an account on a social networking site, condition 34 also prohibits defendant from purchasing, possessing, controlling, or having access to any computer or device with internet capabilities and from maintaining any "internet account," including email, without permission from his probation officer. Condition 35 prohibits defendant from owning, renting, or possessing a cell phone with picture taking capabilities or cameras or video recorders for capturing images. In light of defendant's lack of a prior criminal history and the lack of evidence in the record linking defendant's use of technology to the underlying offense, we conclude that those parts of condition 34 and the entirety of condition 35 do not relate to the goals of probation and thus are not enforceable on that ground (*see generally People v Mead*, 133 A.D.3d 1257, 1258 [4th Dept 2015]). We therefore modify the judgment by striking condition 35 as a condition of probation in its entirety and striking condition 34 as a condition of probation and replacing it with the following condition: 'Probationer shall not use the internet to access pornographic material, shall not access or have an internet account for a commercial social networking website as defined by Penal Law § 65.10 (4-a) (b), and shall not communicate with other individuals or groups for the purpose of promoting sexual relations with persons under the age of 18.'

#Probation and Supervised Release

People v. Sneed, 2021 IL App (4th) 210180 (Nov. 18, 2021)

The defendant was charged with two counts of forgery. The police obtained a warrant to search his cell phone but were unable to do so because it was password-protected and the defendant refused to provide the passcode. The trial court denied the prosecution's motion to compel production of the passcode on Fifth Amendment grounds. The State appealed and the appellate court reversed. Addressing the applicability of the privilege against self-incrimination, the court held that production would not be "testimonial:"

¶ 59 The questions raised in *Stahl* and *Andrews* regarding the continued viability of the key/combination analogy (*i.e.*, mental/physical dichotomy) in the digital age deserve consideration. We, too, observe that a cell phone passcode is string of letters or numbers that an individual habitually enters into his electronic device throughout the day. A passcode may be used so habitually that its retrieval is a function of muscle memory rather than an exercise of conscious thought. A fair question that arises, then, is whether the rote application of a series of numbers should be treated the same as the *Hubbell* respondent's "exhaustive use of the 'contents of his mind'" to produce hundreds of pages of responsive documents. The two scenarios appear to bear no resemblance to each other.

¶ 60 We share the concerns expressed in *Stahl* and *Andrews* and observe that, given the advancements in technology, a cell phone passcode is more akin to a key to a strongbox than a combination to a safe. Or, at the very least, perhaps in this digital age the distinction between a physical key and a combination to a safe has become blurred, with a cellular phone passcode encompassing both. This blurring of distinctions would diminish the analytical value of the analogy that so many courts have relied on to hold that the act of providing a passcode is testimonial.

¶ 61 Moreover, at least one federal court has hinted that the act of unlocking a phone may not be testimonial if (1) no dispute exists that the suspect owns the phone, (2) the suspect is not asked to reveal the passcode to the police, and (3) the suspect makes the contents of her cell phone accessible to the police by entering it herself without telling the police the passcode. See *United States v. Oloyede*, 933 F.3d 302, 309 (4th Cir. 2019) ('[Defendant] has not shown that her act communicated her cell phone's unique passcode. Unlike a circumstance, for example, in which she gave the passcode to an agent for the agent to enter, here she simply used the unexpressed contents of her mind to type in the passcode herself'). In *Oloyede*, the defendant entered the passcode herself and gave the unlocked phone to the police officer. *Id.* at 308. The officer did not ask for the passcode or observe the defendant enter the passcode, and the defendant did not reveal the passcode to the police. *Id.* Similarly, in the case before us, the State is requesting an order that the defendant 'provide entry' to his cell phone. That means that defendant, like the defendant in *Oloyede*, could simply enter his passcode into his phone and thereby make its contents accessible to the police without ever telling the police the passcode.

¶ 62 Notably, the trial court in this case, when ruling on the State's motion, expressed its belief that the facts here were 'no different than

> compelling a Defendant to disclose a key to a storage unit or a lockbox or something of that nature.' The court then observed, 'Here, disclosing the passcode would not seem to make extensive use of the contents of the Defendant's mind' and expressed its opinion that 'an objective, reasonable judge could reach the conclusion that the production of the pass code is not testimonial.' However, the court correctly acknowledged that it was obligated to follow the Third District's holding in *Spicer* that the production of a passcode is testimonial because no other Illinois court of review had yet spoken on the issue.
>
> ¶ 63 For the reasons stated, we conclude that requiring defendant to provide entry or the passcode to the phone does not compel him to provide testimony within the meaning of the fifth amendment.

The appellate court then addressed the foregone conclusion doctrine, holding that it applied:

> ¶ 69 The parties' initial disagreement centers upon whether a court conducting a foregone conclusion analysis should focus on (1) the compelled communication itself (i.e., the entry of the passcode) or (2) the information to be revealed by the entry of the passcode. One scholar has helpfully described these competing focuses as (1) the act that opens the door and (2) the treasure that lies beyond the door. See Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination,* 97 Tex. L. Rev. 767, 777 (2019).
>
> ¶ 70 Courts are also split on this issue. Several courts have held that the proper focus of the foregone conclusion analysis is on the testimonial value of the act of producing the passcode. See *Andrews,* 234 A.3d at 1273 ('[W]e find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents.'); *Stahl,* 206 So.3d at 136 ('[T]he relevant question is whether the State has established that it knows with particularity that the passcode exists, is within the accused's possession or control, and is authentic.'); *Gelfgatt,* 11 N.E.3d at 615 ('[W]e conclude that the factual statements that would be conveyed by the defendant's act of entering an encryption key in the computers are 'foregone conclusions' and, therefore, the act of decryption is not a testimonial communication that is protected by the Fifth Amendment.'); *State v. Johnson,* 576 S.W.3d 205, 227 (Mo. 2019) ('The focus of the foregone conclusion exception is the extent of the State's knowledge of the existence of the facts conveyed through the compelled act of production. Here, [defendant] was ordered to produce the passcode to his phone.'); *Commonwealth v. Jones,* 117 N.E.3d 702, 710 (Mass. 2019) ("[F]or the foregone conclusion exception to apply, the Commonwealth must establish that it already knows the

testimony that is implicit in the act of the required production. [Citation.] In the context of compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device.").

¶ 71 Other courts have placed the focus of the foregone conclusion analysis on the files stored on the device. See *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011,* 670 F.3d at 1346 ("Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives ***."); *Seo v. State,* 148 N.E.3d 952, 958 (Ind. 2020) ('This leads us to the following inquiry: has the State shown that (1) [defendant] knows the password for her iPhone; (2) the files on the device exist; and (3) she possessed those files?'); *G.A.Q.L.,* 257 So.3d at 1063 ('It is not the verbal recitation of a passcode, but rather the documents, electronic or otherwise, hidden by an electronic wall that are the focus of this exception.').

***

¶ 89 Placing the focus of the foregone conclusion doctrine on the passcode rather than the documents or evidence contained on the phone appears to strike the most appropriate balance between fifth amendment concerns and fourth amendment concerns. In this case, the State's motion seeks the compelled production of the passcode. The production of the passcode will lead to the contents of the phone, for which the State has obtained a valid search warrant that defendant does not challenge.

***

¶ 92 The contents of the phone are protected by the fourth amendment, and in this case, the State followed proper procedures to obtain a valid search warrant to seize that information. The testimonial value of the act of producing the passcode-a series of letters or numbers which 'opens the door' to permit the State to execute that valid warrant-must be analyzed separately from the State's authority to seize the evidence on the phone. And it bears repeating that defendant does not challenge the probable cause supporting the search warrant that authorizes seizure of the contents of his phone. Instead, he seeks to utilize the fifth amendment to prevent the operation of the fourth amendment, which authorizes (as here) the issuance of a search warrant based upon a verified complaint showing probable cause for the presence of evidence of a crime in the premises (here, the cell phone) to be searched.

¶ 93 By focusing (1) the fifth amendment analysis on the production of the passcode and (2) the fourth amendment analysis on the evidence

> contained on the phone, one constitutional provision does not become either superior or subservient to the other. Further, doing so ensures that the protection against compelled self-incrimination and the interests of law enforcement in executing a valid search warrant are both respected.
>
> ***
>
> ¶ 98 Applying these principles to the case before us, for the forgone conclusion doctrine to apply, the State must establish with reasonable particularity (1) it knows the passcode exists, (2) the passcode is within the defendant's possession or control, and (3) the passcode is authentic. See *Andrews*, 234 A.3d at 1274-75; *Stahl*, 206 So.3d at 136.
>
> ***
>
> ¶ 101 Last, the courts in *Andrews* and *Stahl* addressed the authenticity element in the context of a cell phone passcode, noting that a passcode is self-authenticating. *Stahl*, 206 So.3d at 136; *Andrews*, 234 A.3d at 1275. That is, if the passcode provides entry to the phone, the passcode is authentic. *Stahl*, 206 So.3d at 136; *Andrews*, 234 A.3d at 1275. Therefore, the authenticity element will be determined when the passcode is entered into the phone.
>
> ¶ 102 Accordingly, the State has shown with reasonable particularity that the passcode exists and is within defendant's possession or control. The passcode will self-authenticate if it unlocks the phone. As such, the foregone conclusion doctrine is satisfied, rendering the act of producing the passcode non-testimonial and outside the protection of the fifth amendment privilege against self-incrimination.

#Fifth Amendment – Self-Incrimination

State v. Acosta, 311 Or. App. 136, 489 P.3d 608 (2021)

The defendant was charged with unlawful delivery of methamphetamine. To prove its case, the State planned to offer screen captures from a detective's cell phone that showed that the defendant had set up the drug sale at a specific location with a Facebook profile that matched his name and picture. The defendant moved to exclude the evidence on authentication and hearsay grounds. The trial court granted the motion. The Court of Appeals reversed:

> This case calls upon us to once again consider issues of authentication of digital evidence, as we recently did in *State v. Sassarini*, 300 Or. App. 106, 452 P.3d 457 (2019). The state challenges the trial court's exclusion of Facebook messages that were purportedly exchanged between defendant and a police detective setting up a methamphetamine delivery.

> The trial court ruled that the messages were inadmissible on two distinct grounds: (1) the state failed to authenticate the messages, and (2) they were hearsay in light of the state's inadequate showing that defendant was the declarant of those out-of-court statements, for purposes of an admission of a party opponent. This case therefore presents an additional question of digital evidence than contained in *Sassarini*: whether the identity of the declarant of a social media post, for purposes of an admission of a party opponent, is a gatekeeping question for the trial court, or is an issue of conditional relevancy to be decided by the jury. We conclude it is the latter, and, as we explain, resolving that issue of identity is accomplished through special jury instructions and, at times, a special verdict form, or an interrogatory verdict form. Here, we agree with the state that it produced sufficient evidence to support a finding that the Facebook account was defendant's and that he was the author of the messages, and we therefore reverse the ruling excluding them.

#Admissibility

#Trial-Related

State v. Burch, 2021 WI 68 (2021)

The defendant appealed from his conviction for first-degree intentional homicide. The homicide investigation shifted focus to the defendant after Fitbit evidence derived from the decedent's boyfriend [Detrie] showed that he had logged only 12 steps around the time of the murder. The Wisconsin Supreme Court affirmed:

> ¶2 First, relying on the Fourth Amendment, Burch moved to suppress the admission of incriminating cell phone data. This data was obtained via an unrelated criminal investigation and kept in a police database. A different law enforcement agency investigating the homicide came upon this data and used it to connect Burch to the homicide. Burch argues that the initial download of the data exceeded the scope of his consent, the data was unlawfully retained, and the subsequent accessing of the data violated his reasonable expectation of privacy. We conclude that even if some constitutional defect attended either the initial download or subsequent accessing of the cell phone data, there was no law enforcement misconduct that would warrant exclusion of that data. Therefore, we conclude the circuit court correctly denied Burch's motion to suppress that data.
>
> ¶3 Regarding the second pre-trial evidentiary motion, Burch asks us to reverse the circuit court's discretionary decision to admit evidence from a Fitbit device allegedly worn by the victim's boyfriend at the time of the homicide. This evidence, Burch maintains, should have been

> accompanied by expert testimony and was insufficiently authenticated. We agree with the State that the circuit court's decision to admit this evidence was not an erroneous exercise of discretion. ***

Addressing the cell phone data, the court held:

> ¶22 In this case, the Sheriff's Office detectives acted by the book. After a DNA sample *** matched Burch, officers checked the interdepartmental records already on file with the police. They discovered the two-month-old Police Department file documenting the investigation for the vehicle related incidents. In it, they found and reviewed Burch's signed consent form and Officer Bourdelais' narrative further documenting Burch's consent. The Sheriff's Office detectives observed that neither the consent form nor the narrative listed any limitations to the scope of consent. And the officers reviewed the downloaded data, having every reason to think it was lawfully obtained with Burch's unqualified consent. [footnote omitted].

The court held that there was no misconduct and that, even if there was "some kind of misconduct, nothing they did would rise beyond mere negligence." Therefore, suppression would be unwarranted under the exclusionary rule.

Turning to the Fitbit evidence, the Supreme Court held that the trial judge did not exceed his discretion in allowing it to be introduced without expert testimony:

> ¶30 In its written order rejecting Burch's argument that expert testimony was required, the circuit court explained that Fitbit's step counters have been in the marketplace since 2009, and the 'principle idea behind pedometers . . . for a significantly longer period than that.' Many smartphones, the court added, 'come equipped with a pedometer by default.' Analogizing to a watch and a speedometer, the court noted that even though the average juror may not know 'the exact mechanics' of a technology's 'internal workings,' the public may nevertheless 'generally understand[] the principle of how it functions and accept[] its reliability.' Similarly, the court reasoned, a Fitbit's use of sophisticated hardware and software does not render it an 'unusually complex or esoteric' technology because the average juror is nevertheless familiar with what a Fitbit does and how it is operated.
>
> ¶31 This conclusion was reasonable and within the circuit court's discretionary authority. The circuit court correctly interpreted the standard for requiring expert testimony and reasonably applied that standard to the Fitbit evidence before it. Given the widespread availability of Fitbits and other similar wireless step-counting devices in today's consumer marketplace, the circuit court reasonably concluded

> Detrie's Fitbit was not so 'unusually complex or esoteric' that the jury needed an expert to understand it. The circuit court's conclusion that expert testimony was not required under these circumstances was within the circuit court's discretion. [footnotes omitted].

The Supreme Court then rejected the defendant's argument that the Fitbit evidence had not been properly authenticated:

> ¶33 *** Burch does not actually disagree that the State's records are accurate copies of Fitbit's records associated with Detrie's Fitbit device. Instead, he focuses his challenge on whether the State properly authenticated 'the information within those records.' Specifically, he argues that 'the State failed to show that the Fitbit device reliably and accurately registered Detrie's steps that evening, and that that data was reliably and accurately transmitted to Fitbit's business records without manipulation.'
>
> ¶34 Burch's argument reaches beyond the threshold question authentication presents. The circuit court's authentication obligation is simply to determine whether a fact-finder could reasonably conclude evidence is what its proponent claims it to be. Wis. Stat. § 909.01. The circuit court did so here by reviewing the Fitbit records and the affidavit of 'a duly authorized custodian of Fitbit's records' averring that the records 'are true and correct copies of Fitbit's customer data records,' and then concluding the data was self-authenticating under Wis. Stat. § 909.02(12). The circuit court's obligation is not to scrutinize every line of data within a given record and decide whether each line is an accurate representation of the facts. Rather, once the circuit court concludes the factfinder could find that the records are what their proponent claims them to be, the credibility and weight ascribed to those records are questions left to the finder of fact. State v. Roberson, 2019 WI 102, ¶25, 389 Wis. 2d 190, 935 N.W.2d 813. The circuit court's conclusion that the Fitbit records were sufficiently authenticated therefore was within its discretion.

#Admissibility

#Fourth Amendment – Warrant Required or Not

#Trial-Related

State v. Caronna, Docket Nos. A-0580-20 & A-0581-20 (N.J. App. Div. Nov.3, 2021)

This appeal required the appellate court to "determine, as a matter of first impression, whether under our State Constitution the exclusionary rule applies to an unconstitutional and flagrant violation of a search warrant's knock-and-announce requirement. A detective requested and obtained a warrant that required the police to knock and announce their presence before entering an apartment." They did not do so. The Appellate Division held that the rule applied:

> We hold that the exclusionary rule applies where police violate Article I, Paragraph 7 by unreasonably and unjustifiably ignoring a search warrant requirement that they knock and announce their presence before entering a dwelling. We also conclude that no exception to the exclusionary rule applies here, especially because of the flagrant violation. *** Compliance with a knock-and-announce warrant requirement is a critical predicate for a reasonable search under our State Constitution. It is simply objectively unreasonable-without justification-for police to ignore a knock-and-announce requirement contained in a warrant that they requested and obtained. Ignoring the requirement contravenes the search and seizure rights of New Jersey residents. Our holding comports with New Jersey's Article I, Paragraph 7 law; effectively deters police from flagrantly violating knock-and- announce search warrant requirements; safeguards against unconstitutional, unreasonable, and illegal searches and seizures under New Jersey law; and, importantly, upholds the rule of law and integrity of our administration of justice. [footnote omitted].

#Fourth Amendment – Good Faith Expectation

#Fourth Amendment – Warrant Required or Not

State v. Carrion, A-14-20 (N.J. Sup. Ct. Dec. 27, 2021)

The defendant was convicted of various offenses. On appeal, he challenged, among other things, the admission of evidence that showed that a non-testifying detective had searched a database that revealed that no permit existed that authorized the defendant to lawfully possess a handgun. The Supreme Court held that that admission of the evidence violated the Sixth Amendment's Confrontation Clause:

> The admitted evidence showed that the non-testifying detective's search of the database revealed no permit existed authorizing Carrion to lawfully possess a handgun when one was seized by police from his home. Applying the test from decisions interpreting the federal Confrontation Clause, which we have adopted in our state confrontation

> jurisprudence, we conclude that, while the raw data contained in the database listing issued firearm permits is not 'testimonial' for purposes of a confrontation-right analysis, statements about the search of that database for information specific to defendant for use in his prosecution is testimonial. Here, the State's reliance on an affidavit by a non-testifying witness to introduce over defendant's objection the results of that search violated defendant's right to confront the witnesses against him.

The Supreme Court went on to explain its ruling:

> To be clear, an affidavit attesting to the absence of a license created after a search of the firearm registry database is distinguishable from a previously existing document that was not created for purposes of an individual defendant's prosecution. An example of the latter, as we held in Wilson, is a map created and maintained by a public entity for official purposes other than prosecution of a specific criminal defendant. See 227 N.J. at 551 (finding that admission of a map, created years before the commission of the alleged offenses and not in response to the criminal event, did not violate the Confrontation Clause). Indeed, another example of a non-testimonial 'document,' as readily conceded by Carrion, is the firearm license database itself. Such raw data, collected for a neutral administrative purpose, is not testimonial. Rather, it is the creation of a document attesting to an interpretation or search of that data -- for the sole purpose of prosecuting a defendant -- that is testimonial.

The court also adopted a new procedure:

> Going forward, however, to help alleviate the administrative concerns of the State, we adopt the practice of notice and demand for the presentation of a State witness to testify to the search of the firearm permit database. Adoption of a notice requirement by which a defendant must inform the court and the State of a demand to have the State produce an appropriate witness will protect a defendant's right to confrontation. See State v. Williams, 219 N.J. 89, 99 (2014). By not demanding the witness's testimony, the defendant waives his confrontation right. See ibid. In many cases, the defendant may conclude that the production of the witness is unnecessary. At the same time, a notice requirement will promote administrative and judicial efficiency. We have adopted such useful practices before and have seen their benefits in other settings that include Crawford considerations. E.g., Wilson, 227 N.J. at 553-54 (creating a notice and demand procedure when a State witness is required to identify, on certified survey maps, the location of seized drugs used in certain drug prosecutions requiring proof of proximity to certain public places or buildings).

#Sixth Amendment – Right of Confrontation

State v. Dawson, 340 Conn. 136 (Conn. 2021)

The defendant was convicted for criminal possession of a handgun. At the time of his arrest, the defendant was sitting in a public place several feet from the weapon with others sitting closer. There was no direct evidence linking him to the weapon. Instead, "only trace amounts of DNA from which defendant's DNA profile could not be excluded was found on the gun, which could not establish that he actually touched the gun." The Appellate Court affirmed. The Connecticut Supreme Court reversed:

> *** the defendant asserts that, without further corroborative proof, the DNA evidence was insufficient as a matter of law to establish his guilt because DNA evidence, standing alone, does not establish that he knowingly exercised dominion or control over the gun. The state counters that the Appellate Court correctly concluded that the cumulative evidence and inferences logically flowing therefrom support the jury's conclusion that the defendant constructively possessed the gun beyond a reasonable doubt. We agree with the defendant.

#Trial-Related

State v. Katz, Supreme Court Case No. 20S-CR-632, 2022 WL 152487 (Ind. Jan. 18, 2022)

> In the modern age of social media, when anyone with a phone can instantaneously publish images worldwide, new potential harms arise unimaginable a generation ago. One such unfortunate phenomenon has come to be known as 'revenge porn.' To punish and deter it, the General Assembly in 2019 enacted Indiana Code section 35-45-4-8, which criminalizes the non-consensual distribution of an 'intimate image.' In this case, Conner Katz—unbeknownst to his girlfriend—captured cell phone video of her performing oral sex on him, then sent it to another person. He was charged under the statute, and in a pre-trial motion to dismiss, challenged its constitutionality on free speech grounds. The trial court dismissed, finding the entire statute violated the state and federal constitutions. The State disagreed and appealed. Katz cross-appealed, arguing we need not reach the question of constitutionality because dismissal should be upheld for failure to state an offense. Because we conclude the State sufficiently alleged an offense, and because we find the statute constitutional, we reverse and remand.

#Miscellaneous

#Social Media

State v. Martinez, No. 13-20-00169-CR (Tex. 13th Dist. Ct. App. Jan. 20, 2022)

The State appealed from the trial court's suppression of a video recording. The video was a "second-hand recording of surveillance footage" originally obtained from rooms in a police department. The recording was made using a cell phone camera and there was a time gap in the recording. The video was used to secure a search warrant for the original footage but it had been automatically erased with the passage of time. The trial court granted a defense motion to suppress because the recording had been "selective[]." The Court of Appeals reversed on interlocutory review, holding that, "there is no rule of evidence or other authority requiring 'the entire thing' to be offered into evidence in order for a part of the whole to be admissible. Instead, whether a video recording is 'complete' goes to the weight of the evidence, not its admissibility." The dissenting judge held that, on the record before the Court of Appeals, the trial judge's decision fell "within the zone of reasonable disagreement and should not be disturbed." (footnote omitted).

#Admissibility

#Trial-Related

State v. McQueen, No. A-11-20 (N.J. Sup. Ct. Aug. 10, 2021)

The defendant was arrested for various offenses and brought to a police station. He was permitted to make a call on one of the station's landlines but was not told that his conversation would be recorded or made available to law enforcement without his consent or a warrant. He called and spoke with the codefendant. After a detective retrieved and listened to their conversation, the codefendant was charged with various crimes. The court below affirmed the suppression of the conversation on Fourth Amendment grounds. The Supreme Court affirmed:

> McQueen's custodial status in the stationhouse did not strip him of all constitutional protections. The police provided McQueen and Allen-Brewer [the codefendant] with no notice that their conversation would be recorded or monitored. Article I, Paragraph 7 [of the New Jersey Constitution], which prohibits unreasonable searches and seizures, broadly protects the privacy of telephone conversations in many different settings. We hold that McQueen and Allen-Brewer had a reasonable expectation of privacy in their conversation in the absence of fair notice

> that their conversation would be monitored or recorded. The recorded stationhouse telephone conversation was not seized pursuant to a warrant or any justifiable exigency and therefore must be suppressed.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

State v. Smith, No. SC99086 (Mo. Jan. 11, 2022) (en banc)

The defendant was convicted on two counts of statutory rape. On appeal, he argued that the trial court had erred in permitting witness testimony via a two-way live video feed because doing so violated his right of confrontation under the United States and the Missouri constitutions. The testimony was given by a crime lab official, who took buccal swabs from the defendant, performed a DNA analysis, and matched the defendant's DNA to that taken from a sexual assault kit. The trial court allowed the "remote" testimony because the official was on paternity leave during the time of the trial. The Missouri Supreme Court reviewed United States Supreme Court decisions which "examine[d] a defendant's right to confront adverse witnesses against him or her when that witness testimony falls short of in-person, face-to-fact confrontation" and concluded:

> Whether the combination of oath, cross-examination, and observation of demeanor, when utilized in a two-way video setting in which the witness is in a remote location with minimal or no safeguards, is ever enough to ensure the reliability of any witness does not have to be decided today because the circuit court made no express finding that Hall was unavailable.
>
> ***
>
> Hall, the witness in the case at bar [the crime lab official], was neither a victim nor a child. The circuit court made no finding that Hall was unavailable. The circuit court's error of admitting Hall's two-way live video testimony was not harmless beyond a reasonable doubt. The testimony from multiple witnesses established I.S. [the alleged victim] recanted her allegations. Absent Hall's testimony, the circuit court ruled the State could not lay a proper foundation to admit the evidence that Smith's DNA matched the DNA from I.S.'s sexual assault kit. This evidence was the only physical evidence proving sexual contact between Smith and I.S. Therefore, the error of admitting Hall's two-way live video testimony was not harmless beyond a reasonable doubt. The circuit court's judgment is reversed, and the case is remanded. [footnote omitted].

#Miscellaneous

#Sixth Amendment – Right of Confrontation

#Trial-Related

In Interest of Y.W.-B., J-39A&B-2021, 2021 WL 6071747 (Pa. Dec. 23, 2021)

At issue here was whether the Pennsylvania Department of Human Services [DHS] had "esablished sufficient probable cause for the trial court to issue an order permitting entry into the home" of the mother of two minor children. DHS had received an anonymous report from unidentified sources that alleged possible neglect by the mother. The report was not introduced into evidence at the hearing below, although DHS summarized the accusations in its petition to allow access. The Supreme Court held that DHS had not established probable cause for the entry order. In so holding, the court rejected DHS' argument that there was a "social worker exception" to the Warrant Requirement of the Fourth Amendment and its Pennsylvania equivalent:

> A child protection home inspection order like the one at issue here is neither a dragnet search nor a search of an individual with a reduced expectation of privacy. It is not a dragnet-type search because it does not involve home visits of all homes in an area for a limited purpose as in *Camara* [*v. Municipal Court*, 387 U.S. 523 (1967)] to inspect wiring. Home visits by DHS are in no sense 'routine and periodic,' but rather must be based upon credible allegations of evidence of neglect occurring in the specified home. Mother likewise has no reduced expectation of privacy in the sanctity of her home based upon any suspicion of potential wrongdoing (like with, e.g., probationers and paroles), and DHS does not rely on the *Griffin* [*v. Wisconsin*, 483 U.S. 868 (1987)] or S*amson* [*v. California*, 547 U.S. 843 (2006] line of cases. As a result, while home visits in the child neglect context are conducted by civil government officials rather than members of law enforcement, they do not fit within the two categories of "administrative searches" entitled to reduced Fourth Amendment and Article 1, Section 8 protections.
>
> ***
>
> We agree that the evidence necessary to establish probable cause in the child neglect context will sometimes be 'different' than is typically presented in a criminal case. For example, a disinterested magistrate in an application for a criminal search warrant cannot consider prior knowledge of the subject of the search. In contrast ***, in a child protective service petition to compel a home visit, the judge presented

> with the petition oftentimes, by design, may have been assigned continuing oversight over matters involving the family whose home is the subject of the inspection. The judge's prior knowledge of the family circumstances will be part of the probable cause analysis. But what is not 'different' is that the evidence necessary to establish probable cause in both settings must be evaluated pursuant to certain basic principles developed primarily in search and seizure jurisprudence (given the abundance of caselaw in this area) – including the existence of a nexus between the areas to be searched and the suspected wrongdoing at issue, an assessment of the veracity and reliability of anonymous sources of evidence, and consideration of the age of the facts in relation to the facts presented to establish probable cause. These fundamental principles are critical to ensure that a court's finding of probable cause is firmly rooted in facts that that support a constitutional intrusion into a private home.
>
> We expressly hold that there is no 'social worker exception' to compliance with constitutional limitations on an entry into a home without consent or exigent circumstances. While most often applied with respect to the police, the United States Supreme Court has ruled that '[t]he basic purpose of [the Fourth] Amendment ... is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.' *New Jersey v. T.L.O.*, 469 U.S. 325, 335 (1985) (emphasis added). As a result, the Fourth Amendment applies equally whether the government official is a police officer conducting a criminal investigation or a caseworker conducting a civil child welfare investigation. ***

#Fourth Amendment – Warrant Required or Not

DECISIONS – FOREIGN

Big Brother Watch v. United Kingdom, Apps. Nos. 58170/13, 62322/14 and 24960/15 (European Ct. of Human Rights: May 25, 2021), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}

#International

#Reasonable Expectation of Privacy

Press Release, *EDPS Orders Europol to Erase Data Concerning Individuals with No Established Link to a Criminal Activity* (Jan. 10, 2022), https://edps.europa.eu/press-publications/press-news/press-releases_en

#International

#Reasonable Expectation of Privacy

STATUTES, REGULATIONS, ETC. – FEDERAL

"2020 Wiretap Report: Intercepts and Convictions Decrease" (United States Courts: June 28, 2021), https://www.uscourts.gov/news/2021/06/28/2020-wiretap-report-intercepts-and-convictions-decrease

#CSLI

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

General Accounting Office, "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," GAO-21-518 (June 2021), https://www.gao.gov/assets/gao-21-518.pdf

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Department of Justice, "Body-Worn Camera Policy" (Office of the Deputy Attorney General: June 7, 2021), https://www.justice.gov/dag/page/file/1402061/download

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Department of Justice, "Cellular Analysis & Geo-Location Field Resources Guide" (FBI CAST: Current as of Mar. 2019), https://www.documentcloud.org/documents/21088576-march-2019-fbi-cast-cellular-analysis-geo-location-field-resource-guide

#Admissibility

#CSLI

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Department of Justice, "Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities" (Office of Public Affairs: Apr. 13, 2021), https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Department of Justice, "United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime" (Office of Public Affairs: Dec. 15, 2021), https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime

#Fourth Amendment – Warrant Required or Not

#International

#Miscellaneous

C.A. Theohary, "Use of Force in Cyberspace," *In Focus* (Cong. Research. Serv.: Dec. 10, 2021), https://crsreports.congress.gov/product/pdf/IF/IF11995

#Miscellaneous

STATUTES, REGULATIONS, ETC. – STATE

Office of the Inspector General, "The Chicago Police Department's Use of Shotspotter Technology" (City of Chicago: Aug. 24, 2021), https://igchicago.org/2021/08/24/the-chicago-police-departments-use-of-shotspotter-technology/

#Admissibility

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

"Protecting Household Privacy Act," Pub. Act 102-0597 (Illinois: Enacted Aug. 27, 2021, eff. date Jan. 1, 2022), Illinois General Assembly - Full Text of Public Act 102-0597 (ilga.gov)

#Fourth Amendment – Warrant Required or Not

#Miscelllaneous

#SCA

"An Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials," L.D. 1585 (Maine: Enacted June 30, 2021, eff. date Oct. 1, 2021), http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1174&item=2&snum=130

#Admissibility

#Discovery

#Fourth Amendment

#Miscellaneous

ARTICLES

B. Ashworth, "Citizen's New Service Helps Paying Users Summon the Cops," *WIRED* (Aug. 3, 2021), https://www.wired.com/story/citizen-protect-subscription/#:~:text=Citizen%2C%20the%20app%20that%20tracks%20local%20crime%20and,security%20agents%20for%20help%20whenever%20they%20feel%20threatened

#Fourth Amendment – Warrant Required or Not

J. Bambauer, "Geofence Warrants are the Future (and That's a Good Thing," *The Volokh Conspiracy* (Mar. 16, 2022), "Geofence Warrants Are the Future (and That's a Good Thing)" (reason.com)

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Miscellaneous

T. Brewster, "Cops Demand Google Data on Anyone Who Searched a Person's Name … Across a Whole City," *Forbes* (May 17, 2017),

https://www.forbes.com/sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/?sh=4011357ade85

#Discovery Materials

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

T. Brewster, "Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address, and Telephone Number," *Forbes* (Oct. 4, 2021), https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=ae7eb9a7c971

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Miscellaneous

B.D. Brown, "Why Did the Trump DOJ Secretly Seize Phone Records from *Post* Journalists?" *Columbia J. Review* (May 12, 2021), https://www.cjr.org/opinion/trump-doj-washington-post-phone-records.php

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

J. Cox, "FBI's Backdoored Anom Phones Secretly Harvested GPS Data Around the World," *Motherboard* (Jan. 4, 2022), FBI's Backdoored Anom Phones Secretly Harvested GPS Data Around the World (vice.com)

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

H.B. Dixon, Jr., "Cell Phones, Social Media, and the Capitol Insurrection," *Judges' Journal* (ABA: Apr. 21, 2021),

https://www.americanbar.org/content/dam/aba/publications/judges_journal/vol60no2-jj2021-tech.pdf

#Admissibility

#Discovery Materials

#Miscellaneous

#Reasonable Expectation of Privacy

#Trial-Related

R. Fausset & G.M. Nieto del Rio, "As Body Cameras Become Commonplace, a Debate Over When to Release the Footage," N.Y. Times (May 2, 2021), https://www.nytimes.com/2021/05/02/us/police-body-cameras-andrew-brown-north-carolina.html#:~:text=As%20body-worn%20cameras%20have%20become%20more%20commonplace%2C%20and,fatal%20encounters%20between%20law%20enforcement%20officers%20and%20citizens

#Admissibility

#Discovery Materials

#Miscellaneous

#Reasonable Expectation of Privacy

#Trial-Related

C. Fennessy, "A Multilateral Surveillance Accord: Setting the Table," *Lawfare* (Lawfare Institute: Apr. 23, 2021), https://www.lawfareblog.com/multilateral-surveillance-accord-setting-table

#Discovery Materials

#Miscellaneous

#Reasonable Expectation of Privacy

#Trial-Related

J. Garland, *et al.*, "Federal Court Expresses Skepticism About Validity of Geofence Warrants But Declines Suppression Remedy," *Covington Inside Privacy*

(Mar. 9, 2022), Federal Court Expresses Skepticism About Validity of Geofence Warrants But Declines Suppression Remedy | Covington Blogs

#CSLI

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

S. Goldenberg & J. Anuta, "Adams Eyes Expansion of Highly Controversial Police Surveillance Technology," *Politico* (Feb. 8, 2022), Adams eyes expansion of highly controversial police surveillance technology - POLITICO

#Miscellaneous

S. Gordon, "DC Court Is Wrong on Jan. 6 Grand Jury Evidence Sharing," *Law360* (July 30, 2021), https://www.law360.com/articles/1408120/dc-court-is-wrong-on-jan-6-grand-jury-evidence-sharing

#Discovery Materials

#Miscellaneous

#Trial-Related

P.W. Grimm, M.R. Grossman & G.V. Cormack, "Artificial Intelligence as Evidence," 19 *Nw. J. Tech. & Intell. Prop.* 9 (2021), https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2

#Admissibility

#Trial-Related

P.W. Grimm, "New Evidence Rules and Artificial Intelligence," *Litigation*, Vol. 45, No.1 (ABA: Fall 2018), New Evidence Rules and Artificial Intelligence (americanbar.org)

#Admissibility

#Trial-Related

S. Holder & F. Akinnibi, "Suburbs of Surveillance," *Bloomberg CityLab* (Aug. 4, 2021), https://www.bloomberg.com/news/features/2021-08-04/surveillance-startup-brings-police-tech-to-neighborhoods

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Trial-Related

V. Hughes, "Two New Laws Restrict Police Use of DNA Search Methods," *N.Y. Times* (May 31, 2021), https://www.nytimes.com/2021/05/31/science/dna-police-laws.html

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Trial-Related

A. Iftimie, "No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims," *Lawfare* (Apr. 19, 2021), https://www.lawfareblog.com/no-server-left-behind-justice-departments-novel-law-enforcement-operation-protect-victims

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Trial-Related

A. Kabaria & J.D. Seiver, "Illinois 'Protecting Household Privacy Act' Takes Effect," *Privacy & Security Law Blog* (Davis Wright Tremaine LLP: Jan. 13, 2022), Illinois "Protecting Household Privacy Act" Takes Effect | Davis Wright Tremaine LLP - JDSupra

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#SCA

O.S. Kerr, "The Fourth Amendment and Geofence Warrants: A Critical Look at *United States v. Chatrie," The Volokh Conspiracy* (Mar. 11, 2022), The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie (reason.com)

#CSLI

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Third-Party Doctrine

O.S. Kerr, "The Fourth Amendment Limits of Internet Content Preservation," 65 *St. Louis Univ. L. J.* 753 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3751094

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Preservation and Spoliation

#Trial-Related

M. MacCarthy, "Mandating Fairness and Accuracy Assessments for Law Enforcement Use of Facial Recognition Systems," *TechTank* (Brookings: May 26, 2021), https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/

#Admissibility

#Discovery Materials

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Trial-Related

R. Mann, "Diverse Six-Justice Majority Rejects Broad Reading of Computer-Fraud Law," *SCOTUSblog* (June 3, 2021), https://www.scotusblog.com/2021/06/diverse-six-justice-majority-rejects-broad-reading-of-computer-fraud-law/

#Miscellanous

M. Mermelstein, S. Frase & A. Epperson, "Overbroad Searches and Seizures: Google Customer Data Stored Outside of Gmail," *Litigation J.* 49 (ABA: fall 2021), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2021-22/fall/overbroad-searches-and-seizures-google-customer-data-stored-outside-gmail/

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

N. Mott, "FBI Document Shows How Popular Secure Messaging Apps Stack Up," *PC* (Nov. 29, 2021), https://www.pcmag.com/news/fbi-document-shows-how-popular-secure-messaging-apps-stack-up

#Miscellaneous

#Reasonable Expectation of Privacy

J. Nash, "Fingerprint Biometrics Still a Solid Tool for Police – Despite Persistent Myths," *BIOMETRIC Update.Com* (Nov. 17, 2021), https://www.biometricupdate.com/202111/fingerprint-biometrics-still-a-solid-tool-for-police-despite-persistent-myths

#Admissibility

#Discovery Materials

#Miscellaneous

#Trial-Related

C.F. Ortiz & K. Suominen, "DOJ and IRS' Analysis of Crypto Records and Work with Private Experts and International Partners Leads to Arrest," *Tax Controversy 360* (Apr. 30, 2021), https://www.taxcontroversy360.com/2021/04/doj-and-irs-analysis-of-crypto-records-and-work-with-private-experts-and-international-partners-leads-to-arrest/

#Admissibility

#Discovery Materials

#Miscellaneous

S.M.G. Rankin, "*Technological Tethereds:* Potential Impact of Untrustworthy Artificial Intelligence in Criminal Justice Risk Assessment Instruments," 78 *Wash. & Lee L. Rev.* 647 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662761

#Admissibility

#Discovery Materials

#Miscellaneous

#Trial-Related

T. Riley, "Feds' Spending on Facial Recognition Tech Expands, Despite Privacy Concerns," *Cyberscoop* (Jan. 10, 2022), https://www.cyberscoop.com/feds-spending-on-facial-recognition-tech-continues-unmitigated-despite-privacy-concerns/

#Admissibility

#Discovery Materials

#Miscellaneous

#Reasonable Expectation of Privacy

#Trial-Related

S. Rippy & N. Sakin, "Van Buren: The Implications of What is Left Unsaid," *Privacy Advisor* (IAPP: June 18, 2021), https://iapp.org/news/a/van-buren-the-implications-of-what-is-left-unsaid/

#Miscellaneous

S.W. Smith, "The Cell Phone Donut Hole in the Tracking Device Statute," 14 *Fed. Cts. L. Rev.* 1 (FMJA: 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3919144

#CSLI

#Miscellaneous

#SCA

M. Tokson, "The Aftermath of *Carpenter*: An Empirical Study of Fourth Amendment Case Law, 2018-2021," 135 Harvard L. Rev. ___ (2021)

(forthcoming), https://gpsbydesigncentre.com/wp-content/uploads/2021/09/SSRN-id3932015.pdf

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Third-Party Doctrine

A.Vittorio, "Robbery Poses Legal Test for Police Use of Google Location Data," *Bloomberg Law News* (Sept. 14, 2021), https://news.bloomberglaw.com/privacy-and-data-security/robbery-poses-legal-test-for-police-use-of-google-location-data

#CSLI

#Fourth Amendment – Warrant Required or Not

D.C. Weiss, "Judge Permits Prosecutors to Use Facial Recognition to Open Accused Capitol Rioter's Laptop," *ABA J. Daily News* (July 23, 2021), https://www.abajournal.com/news/article/judge-permits-prosecutors-to-use-facial-recognition-to-open-accused-capitol-rioters-laptop

#Fifth Amendment – Self-Incrimination

Z. Whittaker, "Google Says Geofence Warrants Make Up One-Quarter of All US Demands," *TechCrunch* (Aug. 19, 2021), https://techcrunch.com/2021/08/19/google-geofence-warrants/

#CSLI

#Discovery Materials

#Miscellaneous

#Reasonable Expectation of Privacy

RJH "final" 2/4/22